ウェブサイト攻撃の検出ツール
「iLogScanner V3.0」

ウェブサーバのアクセスログを解析して

脆弱性を狙った攻撃の検出を簡易に行うツール

取扱説明書

IPA® 独立行政法人 情報処理推進機構
セキュリティセンター

2010 年 8 月

目次

1. はじめに 1
1.1. このプログラムの目的 1
1.2. 機能概要 1
1.3. 解析対象のウェブアプリケーション攻撃 1
1.3.1 各脆弱性の説明 2
2. 動作環境について 4
2.1. 動作環境 4
2.2. ウェブブラウザの設定 5
2.3. Javaの設定 7
2.4. アプレットへの署名確認 8
2.5. アクセスログファイル形式 8
2.6. エラーログファイル形式 13
3. iLogScanner基本操作 14
3.1. 初期画面表示 14
3.2. アクセスログファイルの設定 15
3.3. 解析結果出力先ディレクトリの指定 16
3.4. オプション設定 17
3.5. 解析開始 21
3.6. 解析終了 23
3.7. 解析結果レポート 25
3.8. 解析結果ログ 27
4. iLogScanner ModSecurity 対応機能 28
4.1. 初期画面表示 28
4.2. 解析対象ファイルの指定 29
4.3. 解析結果出力先ディレクトリの指定 30
4.4. オプション指定 30
4.5. 解析開始 31
4.6. 解析終了 34
4.7. 解析結果レポート 36
4.8. 解析結果ログ 37
4.9. ログ統計情報レポート出力機能 39
5. FAQ 44
5.1. iLogScannerとは何ですか？ 44
5.2. iLogScannerは無料で使用できるのですか？ 44

5.3. iLogScannerが検出できるウェブアプリケーション攻撃の種類を教えてください。 44
5.4. iLogScannerが動作する環境を教えてください。 45
5.5. 攻撃と思われる痕跡はどのように検出しているのですか？ 47
5.6. 解析レベルを「詳細」に設定したときに行われる「攻撃が行われている可能性」はどのように検出しているのですか？ 48
5.7. 攻撃が成功した可能性が高い痕跡はどのように検出しているのですか？ 49
5.8. 解析結果で攻撃があったと思われる痕跡が検出されたのですが、どうすればよいですか？ 49
5.9. 解析することができるエラーログを出力するModSecurityのバージョンは？ 50
5.10. 攻撃があったと思われる件数があるのに、その内、ModSecurityで検出・遮断した件数が 0 件なのですがどうしてでしょうか？ 50
5.11. Javaアプレット画面が表示されませんが、何が原因と考えられますか？ 51
5.12. 実行中、「入力されたログフォーマットが不正です。」という旨のメッセージが表示されます。どうすればよいですか？ 51
5.13. 実行中、「指定されたディレクトリは、存在しないか書き込み権限がありません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？ 51
5.14. 実行中、「メモリが不足しています」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？ 52
5.15. 実行中、「システムエラーが発生しました」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？ 52
5.16. 実行画面の表示で英数字以外の文字が全て"□"で表示されてしまいます。どうすればよいですか？利用環境は、Vline Linux4.2/FireFox2.0/JRE5 です。 52
5.17. iLogScannerが動作しません。利用環境は、WinXP/Firefox/JRE6 です。どうすればよいですか？ 52
5.18. 「SQLインジェクションによるホームページ改ざん行為」はiLogScannerで検出できるでしょうか？ 52
5.19. 検査結果などのデータをIPAに送信していますでしょうか？ 52
5.20. 実行中、「ファイルまたはディレクトリが存在していません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？ 52
5.21. 実行中、「入力ファイルのログタイプ形式が不正です。」という旨のメッセージが表示され、解析処理が行われません。どうすればよいですか？ 53
5.22. 実行中、「入力ファイルに必須のカラムデータが存在していません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？ 53
5.23. 実行中、「当ツールを実行する許可が取消しされました。」という旨のメッセー

ジが表示され、処理が中止されました。どうすればよいですか？ 53
5.24. 解析にはどのくらい時間がかかりますか？ 53
5.25. 今回のバージョンアップで追加した機能は何ですか。 54
6. Tips集 56
6.1. VlineLinux4.2 + FireFox2.0 +JRE5 においての文字化け対応 56
6.2. IIS7.0 でのW3Cフィールとの設定方法について 56

1. はじめに

1.1. このプログラムの目的

IPA では、ウェブアプリケーションに対してどれほどの攻撃を受けているのか、ウェブサイト管理者が簡単に状況を把握できる手段を提供していく必要があると考えています。そこで、ウェブサイトのアクセスログを解析することで、そのサイトへの攻撃痕跡を確認でき、一部の痕跡に関しては攻撃が成功した可能性を確認できるツール「iLogScanner」を開発しました。ウェブサイトへの攻撃が成功した可能性が確認された場合は、ウェブアプリケーションに潜む脆弱性を確認する事ができると共に、インターネットに公開しているウェブサイトがどれほど危険であるかを認知してもらい、ウェブサイト管理者や経営者に対して警告を発し、対策を講じるきっかけとなる事が期待できます。

1.2. 機能概要

iLogScannerおよびiLogScanner ModSecurity*対応機能は、利用者がウェブブラウザを利用してIPAのウェブサイトからダウンロードし、利用者のウェブブラウザ上で実行するJavaアプレット形式のプログラムです。

iLogScanner は、利用者が用意したウェブサーバのアクセスログファイルを解析し、ウェブアプリケーションへの攻撃の有無を解析結果レポートとして出力します。

iLogScanner ModSecurity 対応機能は、利用者が用意したウェブサーバの Apache アクセスログファイルおよび ModSecurity のエラーログファイルを解析し、ウェブアプリケーションへの攻撃の有無を解析結果レポートまたは統計情報レポートとして出力します。

1.3. 解析対象のウェブアプリケーション攻撃

iLogScanner は、次の脆弱性を狙ったウェブアプリケーション攻撃の痕跡と攻撃が成功した可能性を検出します（2010 年 05 月現在）。

【ウェブアプリケーション攻撃の痕跡と攻撃が成功した可能性を検出】

- SQL インジェクション

【ウェブアプリケーション攻撃の痕跡を検出】

- OS コマンド・インジェクション
- ディレクトリ・トラバーサル
- クロスサイト・スクリプティング

* ModSecurity：Breach Security社が提供するWAFの機能を有するソフトウェア

- その他（IDS*回避を目的とした攻撃）

【詳細レベルの検出対象】

- 同一 IP アドレスから同一 URL に対する攻撃の可能性
- アクセスログに記録されない SQL インジェクションの兆候
- Web サーバの設定不備を狙った攻撃の可能性

1.3.1　各脆弱性の説明

・「SQL インジェクション」とは

データベースと連携したウェブアプリケーションに問合せ命令文の組み立て方法に問題があるとき、ウェブアプリケーションへ宛てた要求に悪意を持って細工された SQL 文を埋め込まれて（Injection）しまうと、データベースを不正に操作されてしまう問題です。これにより、データベースが不正に操作され、ウェブサイトは重要情報などが盗まれたり、情報が書き換えられたりといった被害を受けてしまう場合があります。

・「OS コマンド・インジェクション」とは

ウェブサーバ上の任意の OS コマンドが実行されてしまう問題です。これにより、ウェブサーバを不正に操作され、重要情報などが盗まれたり、攻撃の踏み台に悪用される場合があります。

・「ディレクトリ・トラバーサル」とは、

相対パス記法を利用して、管理者が意図していないウェブサーバ上のファイルやディレクトリにアクセスされたり、アプリケーションを実行される問題です。これらにより、本来公開を意図しないファイルが読み出され、重要情報が盗まれたり、不正にアプリケーションを実行されファイルが破壊されるなどの危険があります。

・「クロスサイト・スクリプティング」とは

ウェブサイトの訪問者の入力をそのまま画面に表示する掲示板などが、悪意あるスクリプト（命令）を訪問者のブラウザに送ってしまう問題です。これにより、アンケート、掲示板、サイト内検索など、ユーザからの入力内容をウェブページに表示するウェブアプリケーションで、適切なセキュリティ対策がされていない場合、悪意を持ったスクリプト（命令）を埋め込まれてしまい、ウェブページを表示した訪問者のブラウザ環境でスクリプトが実行さ

* IDS：侵入検知システム（Intrusion Detection System）

れてしまう可能性があります。その結果として、cookie などの情報の漏洩や意図しないページの参照が行われてしまいます。相対パス記法を利用して、管理者が意図していないウェブサーバ上のファイルやディレクトリにアクセスされたり、アプリケーションを実行される問題です。これらにより、本来公開を意図しないファイルが読み出され、重要情報が盗まれたり、不正にアプリケーションを実行されファイルが破壊されるなどの危険があります。

・「その他（IDS 回避を目的とした攻撃）」とは

１６進コード、親パス等の特殊文字を使用して偽装した攻撃用文字列で攻撃が行われることによりアプリケーションの妥当性チェック機構を迂回し、SQL インジェクション、クロスサイト・スクリプティング等の攻撃を行うことを狙ったものです。また、ワームなどが悪用するウェブサーバの脆弱性を突いた攻撃でも、このような特殊文字が使われます。それぞれの攻撃に応じた対策が必要になります。

・同一 IP アドレスからの攻撃の可能性

同一の IP アドレスからの攻撃痕跡が一定件数に達しています。基準値を超えているため、攻撃を受けている可能性があります。

・アクセスログに記録されない SQL インジェクションの兆候

ウェブサーバが「SQL インジェクション」の攻撃の影響を受けている可能性を示すものです。同一 IP アドレスから行われたリクエストに対するウェブサーバからのエラー応答が、基準値に達しています。

・Web サーバの設定不備を狙った攻撃の可能性

Web サーバの設定不備を狙った攻撃を受けている可能性があります。

対象となる設定不備は以下の通りです。

「PUT メソッドの設定不備」

「FrontPage Server Extensions の設定不備」

「Tomcat の設定不備」

脆弱性については、IPA　セキュリティセンターの「知っていますか？脆弱性（ぜいじゃくせい）」http://www.ipa.go.jp/security/vuln/vuln_contents/index.html で解説が行われていますので、ご参照ください。

2. 動作環境について

2.1. 動作環境

iLogScanner が動作する環境は、以下を想定しています。

CPU	Intel Pentium4 2.8Ghz 以上を推奨
搭載メモリ	1GB 以上を推奨
オペレーティングシステム	Microsoft Windows XP Professional SP2、SP3
ウェブブラウザ	Internet Explorer 7
Java 実行環境（JRE）	Sun Microsystems 社 J2SE Runtime Environment(JRE) 6.0

JRE 6.0 ダウンロードサイトは、http://java.sun.com/javase/ja/6/download.html になります。

その他、以下の環境においては一部動作可能であることを確認しております。

※ 以下に記載した環境での動作を保証するものではございません。オペレーティングシステム/ウェブブラウザ/JREのバージョン、利用者環境等の違いにより、動作が異なる場合もございますので、予めご了承ください（2010 年 05 月現在）。

	オペレーティングシステム	ウェブブラウザ	Java 実行環境（JRE）	動作
1	Microsoft Windows XP Professional SP2	Internet Explorer 6	JRE 6.0	○
2		Internet Explorer 7	JRE 6.0	○
3		Internet Explorer 8	JRE 6.0	○
4		Firefox 3	JRE 6.0	○
5	Microsoft Windows XP Professional SP3	Internet Explorer 6	JRE 6.0	○
6		Internet Explorer 7	JRE 6.0	○
7		Internet Explorer 8	JRE 6.0	○
8		Firefox 3	JRE 6.0	○
9	Microsoft Windows7 Professional	Internet Explorer 8	JRE 6.0	○
10		Firefox 3	JRE 6.0	○
11	Microsoft Windows Vista Business ※1	Firefox 3	JRE 6.0	○
12	Linux(CentOS 5)	Firefox 3	JRE 6.0	△※2

○：正常動作する　△：一部を除き正常動作する　×：正常動作しない

【補足事項】

※1　Windows Vista について

Windows Vista + Internet Explorer　7 では初期設定で「保護モード」が有効となっている為、iLogScanner を正常に動作させることができません。「保護モード」を無効にすると、ブラウザを悪用する不正なソフト（ウイルス、スパイウェア）などの動きを抑えることができなくなってしまいますので、セキュリティの観点から Windows Vista + Internet Explorer　7 上での実行は推奨しておりません。また、Windows Vista はブラウザが Firefox3 であればユーザの権限に関わらず正常動作します。しかし、Internet Explorer 7（保護モード ON）使用時と比較するとセキュリティ性が高くない為、Firefox での実行は推奨していません。

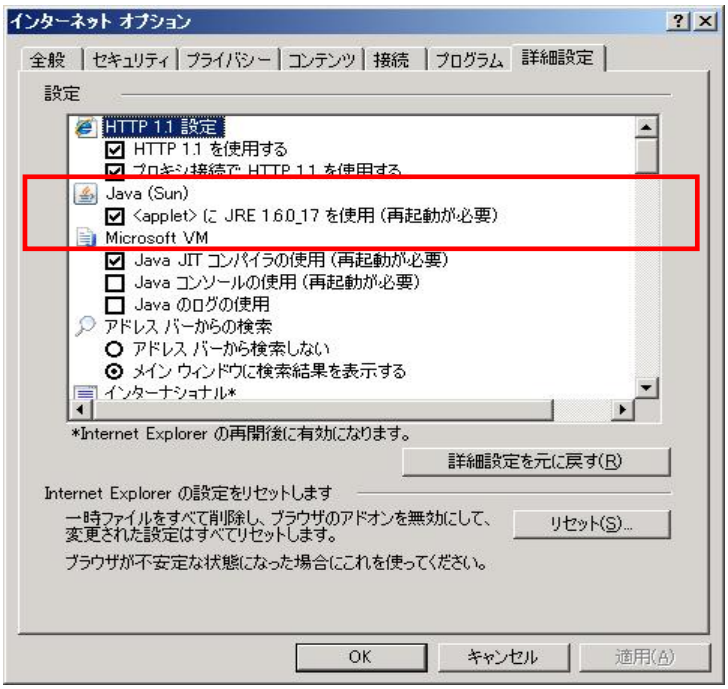
※2　Linux（CentOS 5）の動作について

Linux 上で FireFox3 を使用しツールを実行したところ、ModSecurity 版の解析においてアクセスログとエラーログのマージが行われない現象がありました。（マージの部分で各脆弱性が検出されるはずの「その内、ModSecurity で検出・遮断した件数」が検出されず 0 件になってしまう）ModSecurity 版でのその他の動作（通常解析と統計情報）は正常に動作しております。JRE6.0 になって、Firefox へのプラグインがいままでと変わっていることが影響していると推測されます。そのため、Linux 上での実行は推奨しておりません。

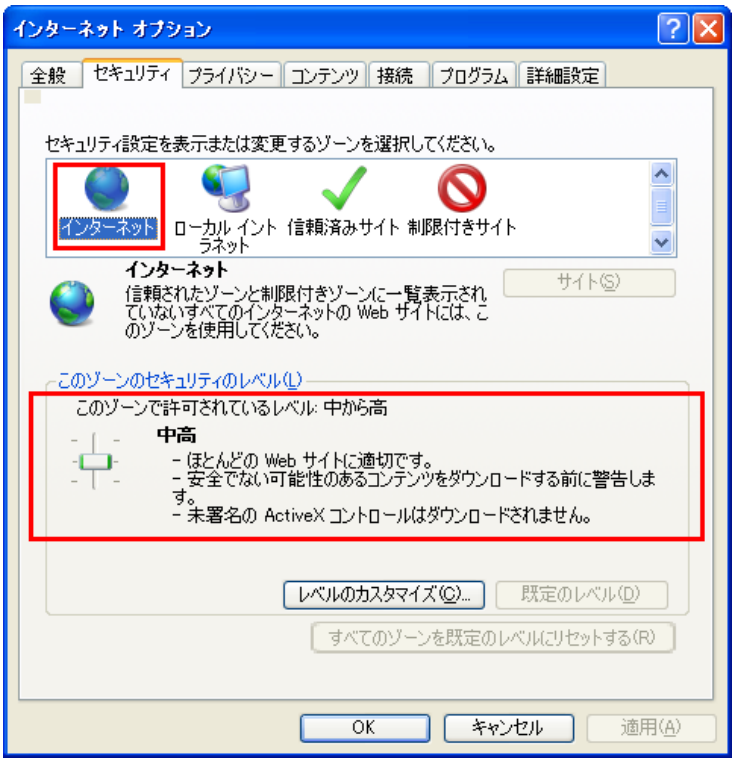
2.2.　ウェブブラウザの設定

Javaアプレットである iLogScannerを実行するために、ウェブブラウザ（Internet Explorer 7）が次の設定になっていることを確認してください。設定を変更する場合は、利用終了後に既存の設定に戻せるように、現在の設定をメモしておき、利用終了後に設定を既存の値に変更してください。また、設定を変更した場合は、Internet Explorer 7 を再起動して設定を反映させる必要があります。

(1)　Internet Explorer 7 のメニューから「ツール」->「インターネットオプション」を開き、「詳細設定」タブの Java の設定項目にチェックが入っていることを確認してください（Sun Microsystems 社 J2SE Runtime Environment(JRE) をインストールすると初期設定でチェックが入っています）。J2SE Runtime Environment(JRE) 6.0 Update 17 がインストールされている場合は、次の画像のようになります。



(2)　「インターネットオプション」の「セキュリティ」タブを開き、『インターネット』ゾーンを選び「このゾーンのセキュリティのレベル」が『中高（既定のレベル)』になっていることを確認してください（Internet Explorer 7 では、インターネットゾーンのセキュリティレベルの初期設定は『中高』になります)。



【補足事項】

「インターネットオプション」の「セキュリティ」の設定で、セキュリティレベル『高』にしている場合、またはセキュリティレベル『高』を基本に「レベルのカスタマイズ」で任意の設定をしている場合、iLogScanner は起動しません。

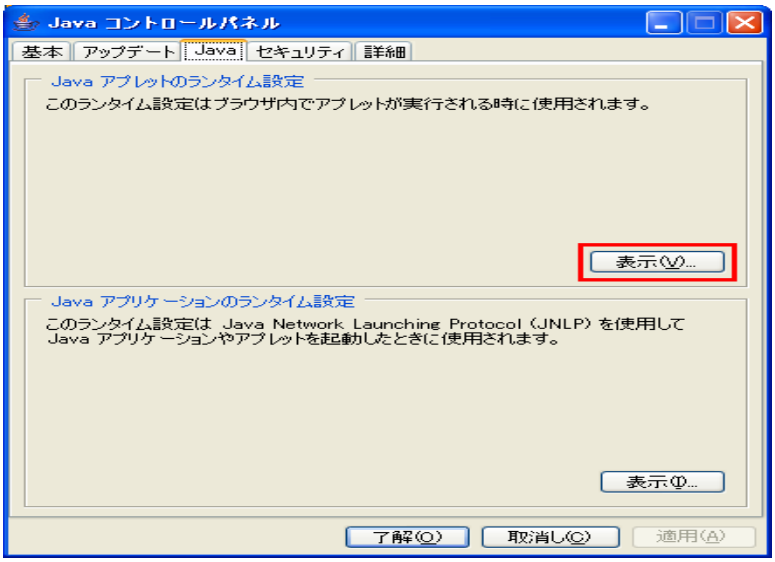
「インターネットオプション」の「セキュリティ」の設定で、『インターネット』ゾーンのセキュリティレベルの設定を変更したくない場合は、『信頼済みサイト』ゾーンを選び「サイト」ボタンをクリックし、信頼済みサイトとして『https://www.ipa.go.jp』を追加した上で、「このゾーンのセキュリティのレベル」を『中高』または『中』にしてください。この設定にした場合は、iLogScanner のウェブページ接続時に『https://www.ipa.go.jp』で接続してください。

2.3. Javaの設定

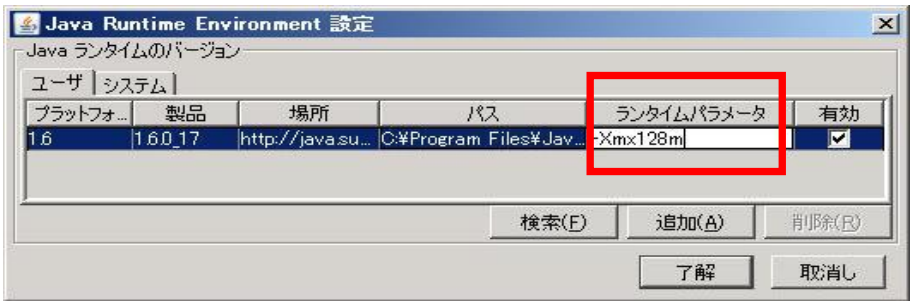
Java に関する設定は、特に必要ありません。

iLogScanner 実行中に、「メモリが不足しています」という旨のエラーメッセージが表示され処理が中止された場合は、次の設定で Java が使用するメモリの最大サイズを大きくしてください（デフォルトでは 64MB です）。

(1) コントロールパネルの「Java」より「Java コントロールパネル」を開きます。「Java 」タブをクリックし、「Java アプレットのランタイム設定」の「表示」ボタンをクリックし、「Java ランタイム設定」画面を開きます。



(2)　「Java ランタイム設定」画面の「Java ランタイムパラメータ」に「-Xmx(size)m」を入力します（下記画像の例は 128MB の場合）。何も入力しない場合（デフォルト）、Java が使用するメモリの最大サイズは 64MB です。



2.4.　アプレットへの署名確認

iLogScanner は電子署名された Java アプレット形式のプログラムです。このため、iLogScanner 実行時に、実行されるアプレットを信頼するかどうかのセキュリティ警告画面が表示されます。

セキュリティ警告画面では、「名前、発行者、ダウンロード元」を確認し、このアプレットが IPA から提供されていることを確認してください。詳細情報を確認する場合は、「証明書の詳細」をクリックし、発行者が信頼される機関であることと有効期限が切れていないことを確認してください。電子署名を確認後は、実行ボタンを押して iLogScanner を実行してください。

注意：セキュリティ警告画面にて実行ボタンが押されなかった場合、iLogScanner は動作しません。

2.5.　アクセスログファイル形式

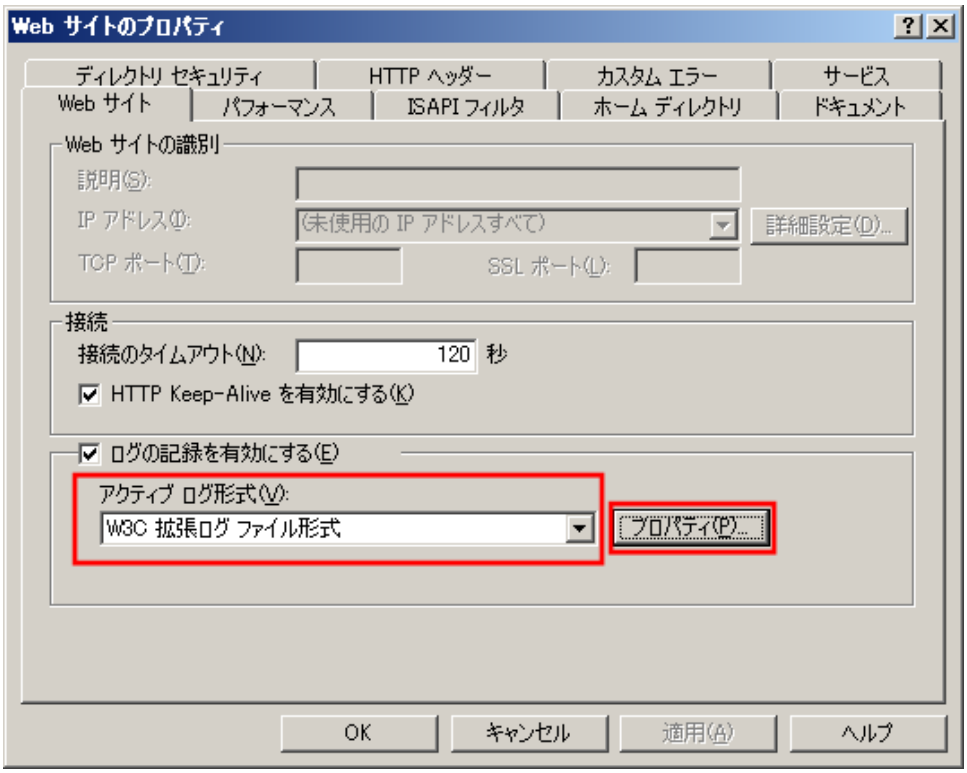
iLogScanner は以下のウェブサーバソフトウェアのアクセスログフォーマットに対応しております。

ウェブサーバソフトウェア	アクセスログフォーマット
Microsoft インターネット インフォメーションサービス(IIS 5.0、5.1、6.0、7.0)	W3C 拡張ログファイル形式
Microsoft インターネット インフォメーションサービス(IIS 5.0、5.1、6.0、7.0)	IIS ログファイル形式
Apache HTTP Server(1.3 系、2.0 系、2.2 系)	Common Log Format

iLogScanner では、アクセスログに出力された GET メソッドのクエリ文字列を解析します。POST メソッドはアクセスログにクエリ文字列が出力されない為、POST メソッドを使用したウェブアプリケーションへの攻撃痕跡の検出には対応しておりません。

(1) W3C 拡張ログファイル形式

「インターネット インフォメーション サービス (IIS) マネージャ」の Web サイトのプロパティより、アクティブ ログ形式が「W3C 拡張ログ ファイル形式」になっている必要があります。



(画面は、IIS6.0 のプロパティになります)

また、アクティブ ログ形式のプロパティにある拡張ログ オプションにおいて次の必須項目が有効になっている必要があります。

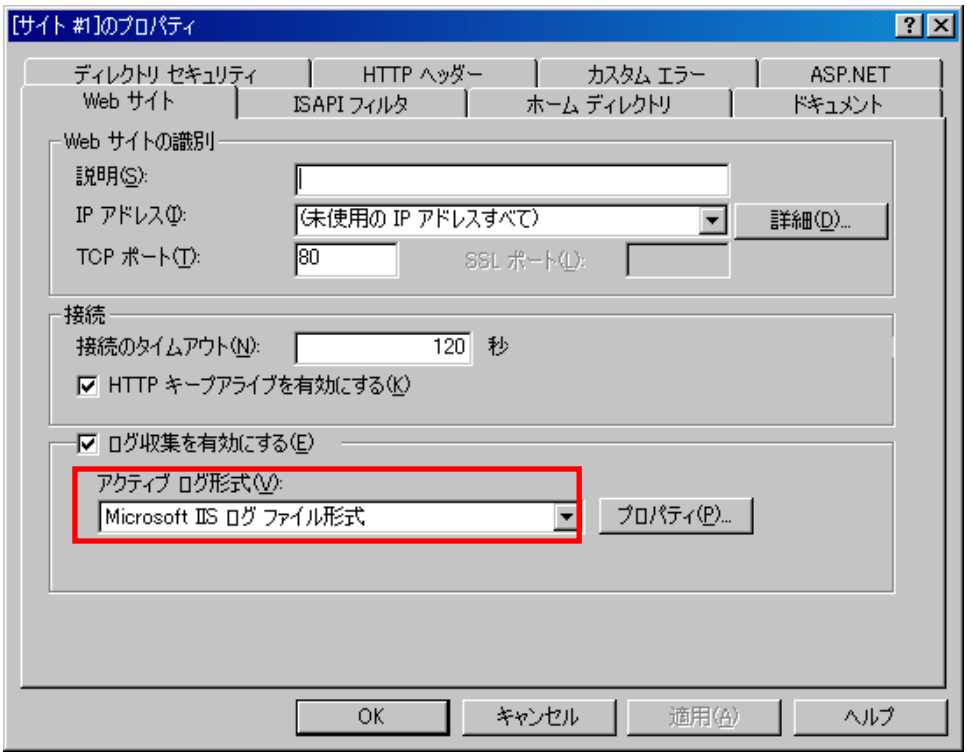
■必須項目

日付(date)
時間(time)
クライアント IP アドレス(c-ip)
ユーザ名(cs-username)
サーバ IP アドレス(s-ip)
サーバポート(s-port)
メソッド(cs-method)
URI Stem(cs-uri-stem)

URI クエリ(cs-uri-query)
プロトコルの状態(sc-status)
ユーザエージェント(cs(User-Agent))

(2)　IIS ログファイル形式

「インターネット インフォメーション サービス (IIS) マネージャ」の Web サイトのプロパティより、アクティブ ログ形式が「Microsoft IIS ログ ファイル形式」になっている必要があります。



（画面は、IIS6.0 のプロパティになります）

以下は IIS5.0/5.1/6.0/7.0 の IIS ログファイル形式のログ項目一覧です。

■IIS5.0/5.1/6.0/7.0 の IIS ログ項目一覧

クライアント IP アドレス
ユーザ名
要求日付
要求時刻
サービス名
サーバ IP アドレス
処理時間
受信バイト数
送信バイト数

サービス状態コード
システム状態コード
メソッド
URI Stem
URI クエリ

(3) Common Log Format

Apache HTTP Server の設定で、Common Log Format（デフォルトで定義されているニックネーム「common」形式）のアクセスログが出力されている必要があります。また、先頭からの書式が Common Log Format と同じ Combined Log Format（デフォルトで定義されているニックネーム「combined」形式）であれば解析することが可能です。

■Apache HTTP Server のアクセスログ出力設定例

```
LogFormat "%h %l %u %t ¥"%r¥" %>s %b" common
CustomLog logs/access_log common
```

■Apache HTTP Server の Common Log Format(CLF)書式

フォーマット文字列	説明
%h	リモートホスト
%l	(identd からもし提供されていれば)リモートログ名
%u	リモートユーザ
%t	リクエストを受付けた時刻。CLF の時刻の書式(標準の英語の書式)。
¥"%r¥"	リクエストの最初の行
%>s	最後のステータス
%b	レスポンスのバイト数。HTTP ヘッダは除く。CLF 書式。

表 2-5-CLF

(4) Apache アクセスログのフォーマット指定

Apache アクセスログのフォーマットが指定できます。そのため、記録項目および順序がカスタマイズされている Apache アクセスログを解析することができます。「表 2-5-CLF」の項目を必須項目と定義とします。また、各項目の区切り文字として「半角スペース」が設定されている必要があります。

入力例）LogFormat "%t %h %l %u ¥"%r¥" %>s %b" common

Apache HTTP Server の設定で設定できる書式指定子（以下の「入力可能な書式指定子」に示す項目）のみ入力可能とします。

【入力可能な書式指定子】

%h　%l　%u　%t　%r　%s　%b　%%　%a %A %B　%C %D

%e %f %i　%m　%n　%o　%p　%P　%q　%T　%U %v　%V　%X　%I　%O

%{Foobar}C　%{Foobar}e　%{Foobar}i　%{Foobar}n　%{Foobar}o

※　Foobar は、「任意の文字列」

2.6. エラーログファイル形式

iLogScanner は以下のウェブサーバソフトウェアのエラーログフォーマットに対応しております。

ウェブサーバソフトウェア	エラーログフォーマット
Apache HTTP Server(2.0 系、2.2 系)	ModSecurity2.5 系が出力するエラーログ形式

(1) ModSecurity2.5 系が出力するエラーログ形式

ModSecurity2.5 系が出力する Apache のエラーログ形式で、ModSecurity の設定で次の必須項目が有効になっている必要があります。

■必須項目

項目概要	例
アクセス日時	Sat Dec 12 11:20:50 2009
Apache のエラーレベル	error
アクセス元 IP アドレス	client 192.168.1.1
タグ	tag “WEB_ATTACK/SQL_INJECTION”
リクエスト URI	uri "/query.php"
リクエストの固有番号	unique_id "Sjr2An8AAAEAABJlx2kAAAAJ"

■ ModSecurity による Apache エラーログの出力例

```
[Sat Dec 12 11:20:50 2009] [error] [client 192.168.1.1] ModSecurity: Warning.
Pattern match "(?:¥¥b(?:(?:s(?:elect¥¥b(?:.{1,100}?¥¥b(?:(?:length|count|top)¥¥
b.{1,100}?¥¥bfrom|from¥¥b.{1,100}?¥¥bwhere)|.*?¥¥b(?:d(?:ump¥¥b.*¥¥bfrom|ata_t
ype)|(?:to_(?:numbe|cha)|inst)r))|p_(?:(?:addextendedpro|sqlexe)c|(?:oacreat|p
repar)e|execute(?:sql)?|makewebtask)|ql_(?...” at ARGS:id. [file "/usr/local/apa
che2/conf/modsec2/modsecurity_crs_40_generic_attacks.conf"] [line "66"] [id "950
001"] [msg "SQL Injection Attack"] [data "or 1="] [severity "CRITICAL"] [tag "WEB_AT
TACK/SQL_INJECTION"] [hostname "centos5.localdomain"] [uri "/query.php"] [unique
_id "Sjr2An8AAAEAABJlx2kAAAAJ"]
```

3. iLogScanner基本操作

iLogScanner は、指定したアクセスログの解析を行い、解析結果を出力します。

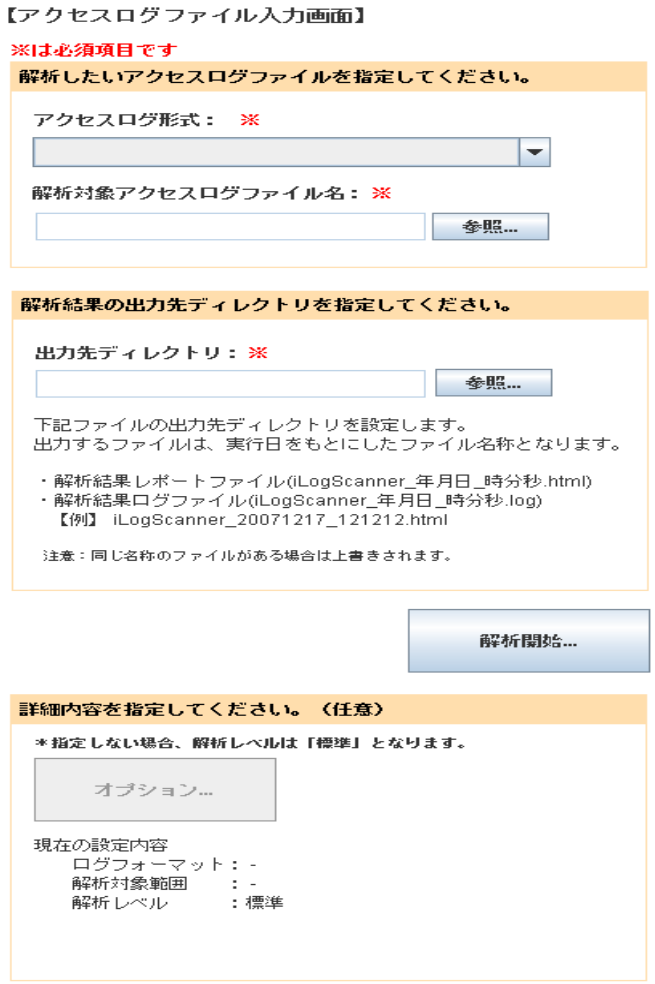
アクセスログ解析のために必要な項目を入力し、解析を実行すると、解析実行中画面が表示され、進捗状況を確認することができます。アクセスログ解析後は、解析結果ファイルを作成し、結果画面が表示されます。

3.1. 初期画面表示

iLogScanner トップページの下部にある「次へ」ボタンを押した後、利用規約ページへ遷移します。利用規約内容を確認し、規約に同意される方は「規約に同意して iLogScanner を起動する」ボタンを押して下さい。

「規約に同意して iLogScanner を起動する」ボタンを押した場合、iLogScanner 初期画面が表示されます。

「規約に同意しない」ボタンを押した場合、iLogScanner トップページへ遷移します。

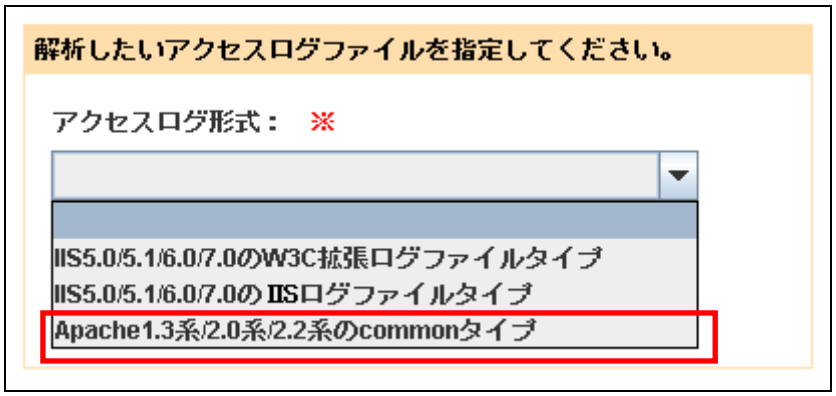


3.2.　アクセスログファイルの設定

解析を行うアクセスログファイルの形式と解析対象ファイルを指定します。
アクセスログについては、「2.5　アクセスログファイル形式」を参照して下さい。

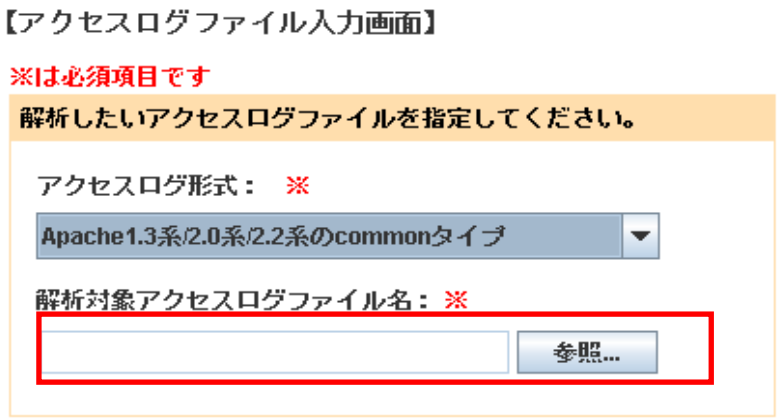
(1)　アクセスログ形式選択

▼ボタンを押してプルダウンを表示し、解析を行うアクセスログファイルのファイル形式を選択します（図はプルダウン表示状態）。

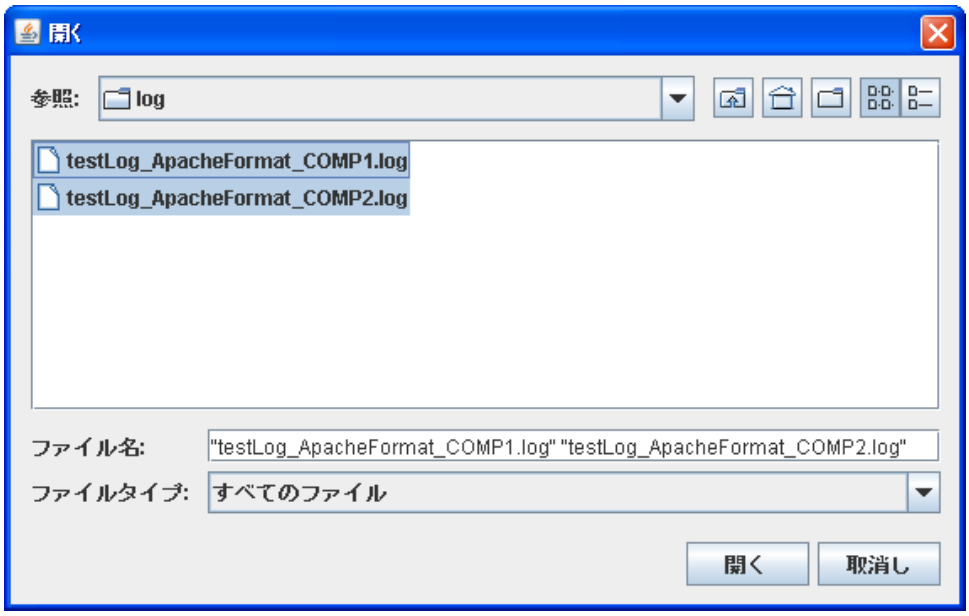


(2)　解析対象アクセスログファイル名選択

「参照」ボタンを押すと、ファイル選択画面が表示されます。



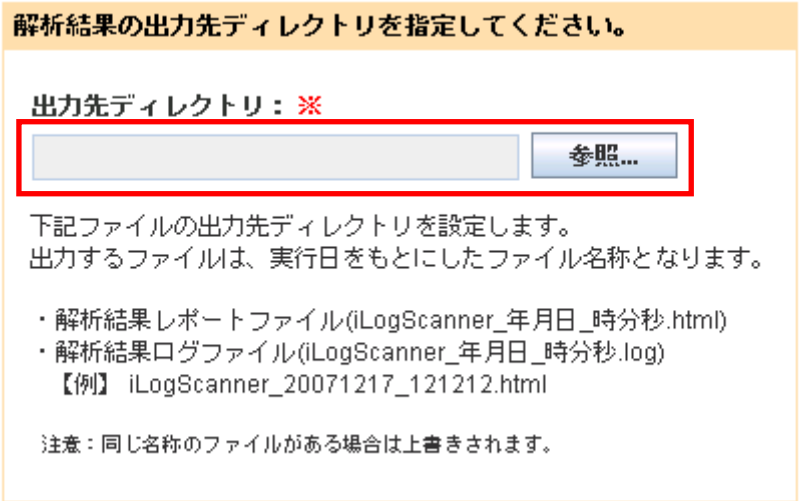
ファイル選択画面にて解析を行うアクセスログファイル名を選択し、開くボタンを押してください。また、アクセスログファイルは複数選択することも可能です。複数選択する場合は、Shift キー(または Ctrl キー)を押しながらファイルを選択します。



3.3. 解析結果出力先ディレクトリの指定

解析結果を出力するディレクトリを指定します。参照ボタンを押すと、ディレクトリ選択画面が表示されます。ディレクトリ選択画面にて、解析結果レポートファイルと解析結果ログファイルの出力先を選択します。解析結果レポートファイル、解析結果ログファイルについては「3.6 解析結果レポート」「3.7 解析結果ログ」を参照して下さい。

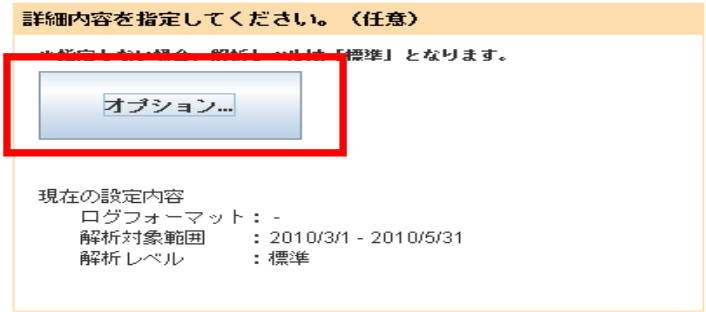
エラー時に出力するエラーログもここで設定したディレクトリに出力されます。出力ディレクトリ設定前にエラーが生じた場合、出力先は実行時のカレントディレクトリになります。



3.4. オプション設定

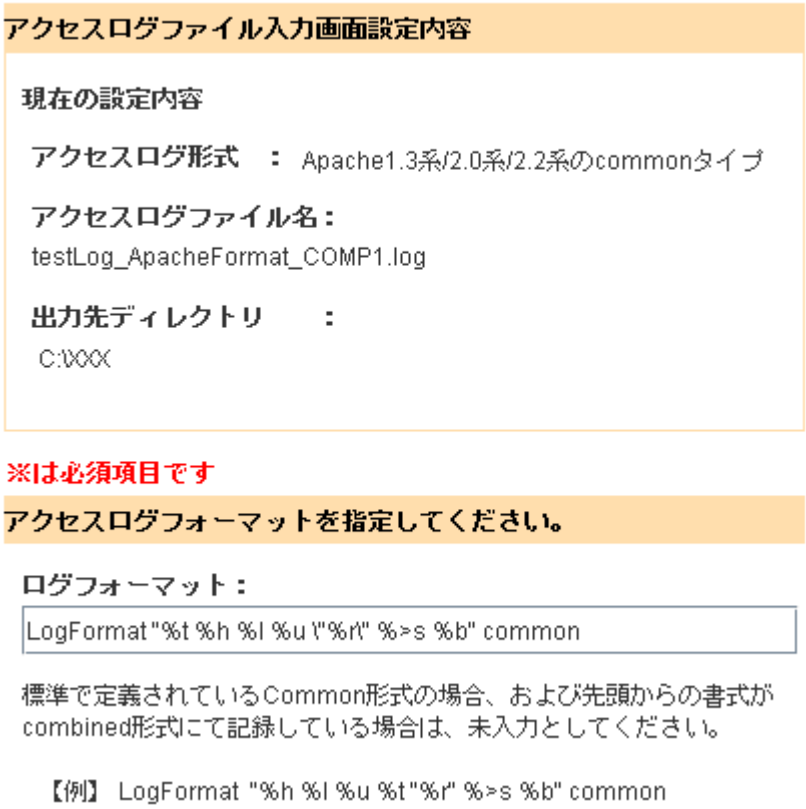
オプション設定では、アクセスログフォーマットの指定、解析対象とする日付の範囲、解析レベルを設定できます。

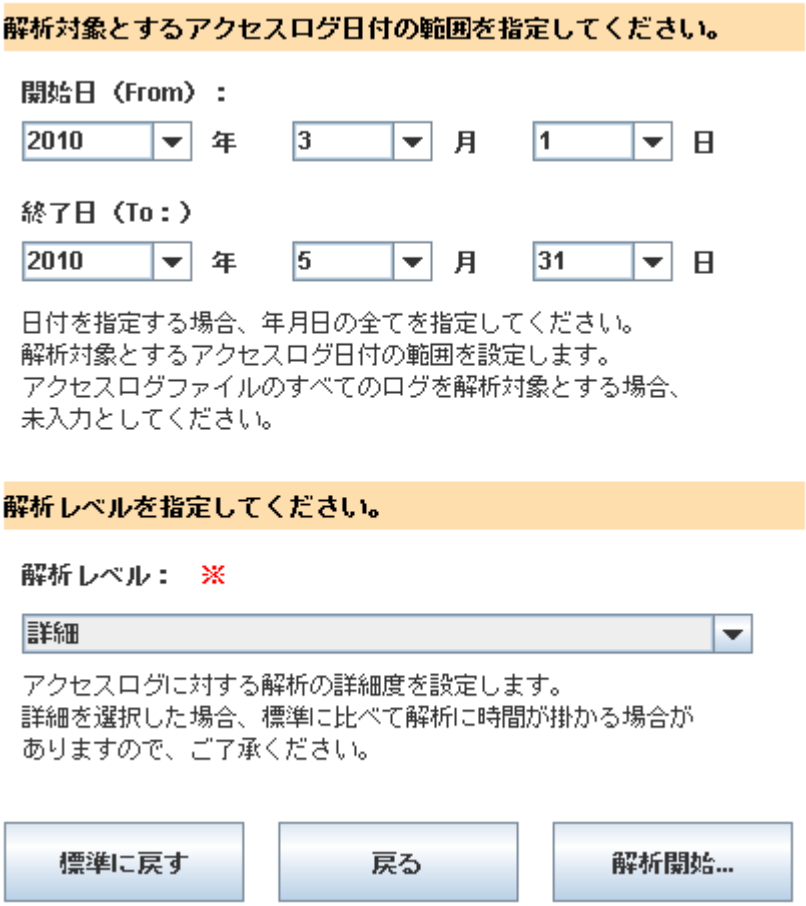
アクセスログファイル形式、解析対象アクセスログファイル、出力先ディレクトリをそれぞれ設定した後、「オプション」ボタンを利用できるようになります。



「オプション」ボタンを押した場合、オプション設定画面が表示されます。

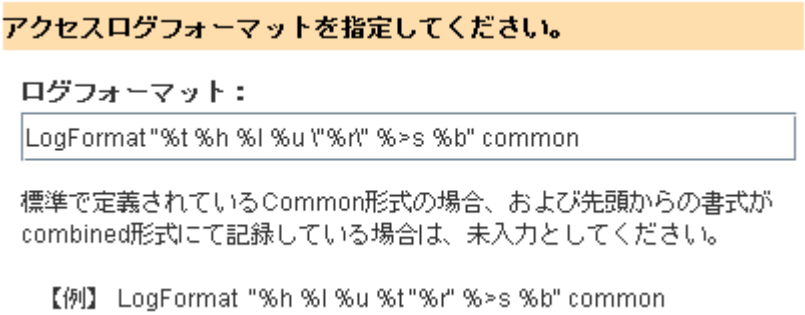
【オプション設定画面】





（1） アクセスログファイルフォーマット設定

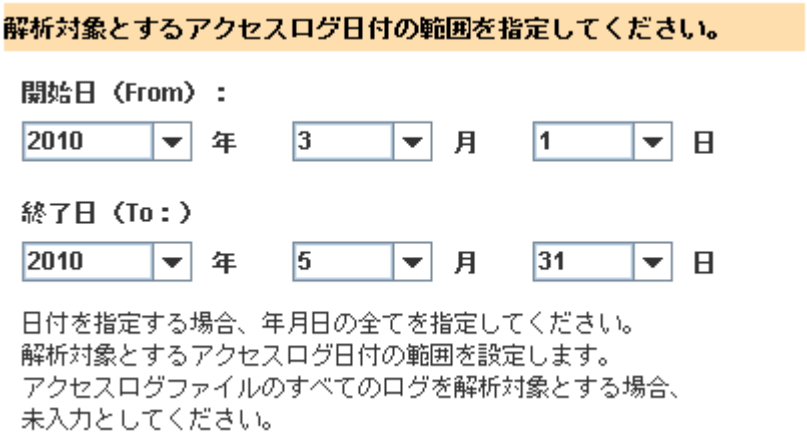
Apache1.3 系、Apache2.0 系、Apache2.2 系の common タイプのみフォーマットを指定できます。



Apache1.3 系/2.0 系/2.2 系にて定義されたフォーマット文字列は「2.5　アクセスログファイル形の(3)の表 2-5-CLF」を参照してください。解析対象として指定されたアクセスログファイルが、設定ログフォーマットと異なる場合、エラーとして処理を行います。

（２） 日付範囲選択

解析対象のアクセスログファイルの日付範囲を指定します。開始日、あるいは終了日のみを指定することができます。



開始日のみ指定した場合、その日からのアクセスログを検出対象とします。
終了日のみ指定した場合、その日までのアクセスログを検出対象とします。
日付を指定しない場合、すべてのアクセスログを検出対象とします。

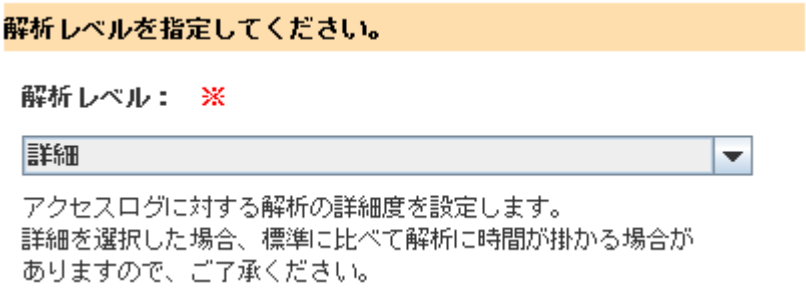
（３） 解析レベル選択

解析対象のアクセスログファイルの解析レベル「標準」「詳細」を選択します。標準レベルの検出対象脆弱性は、以下のとおりです。

- SQL インジェクション
- OS コマンド・インジェクション
- ディレクトリ・トラバーサル
- クロスサイト・スクリプティング
- その他

詳細レベルの検出対象脆弱性は、標準レベルの検出対象脆弱性と、下記の脆弱性が検出されます。

- 同一 IP アドレスからの攻撃の可能性
- アクセスログに残らない SQL インジェクション兆候
- Web サーバの設定不備を狙った攻撃の可能性



（４） 設定解除と画面遷移

「標準に戻す」ボタンを押すと、初期表示の状態に戻します。初期値について、下記のとおりです。

ログフォーマット：空白

開始日：空白

終了日の：空白

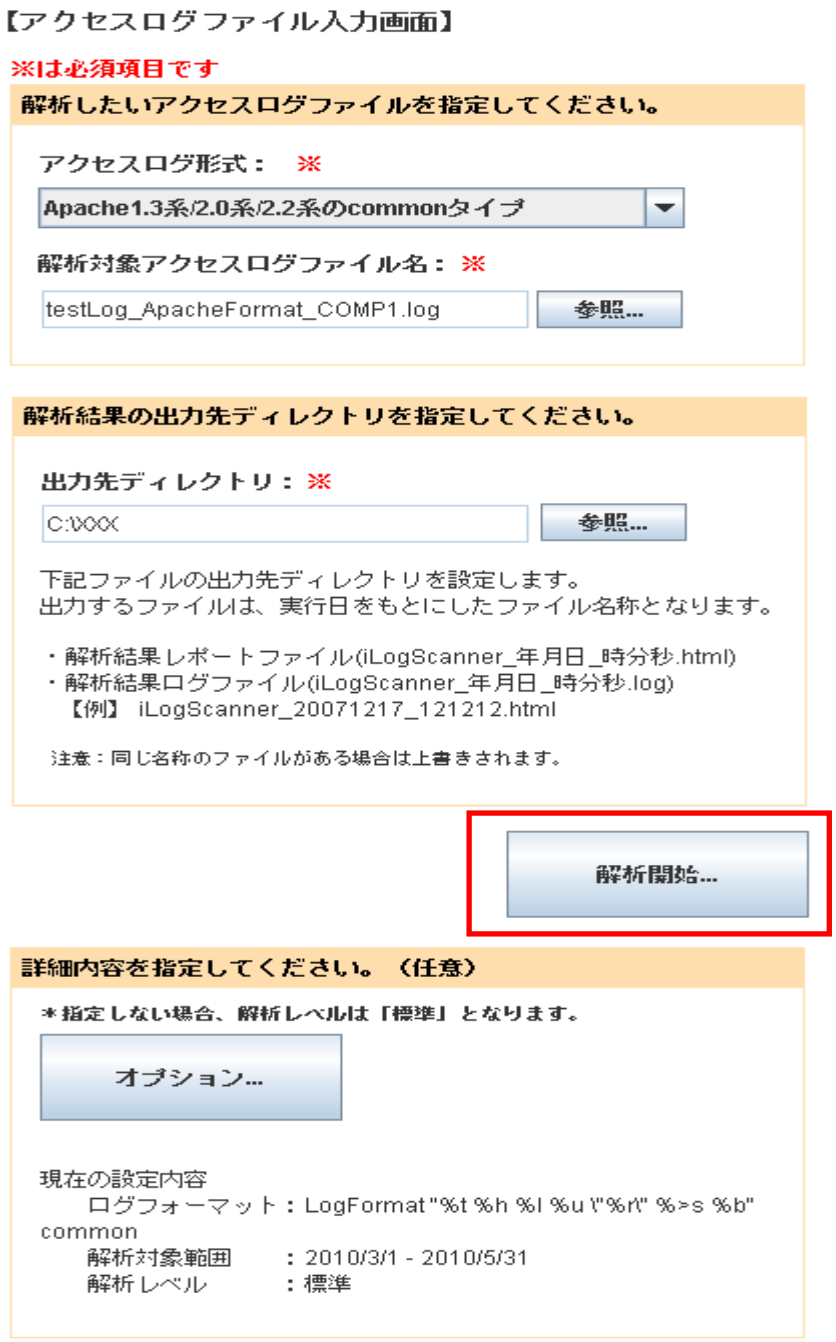
解析レベル：標準

「戻る」ボタンを押すと、アクセスログ入力画面へ遷移します。

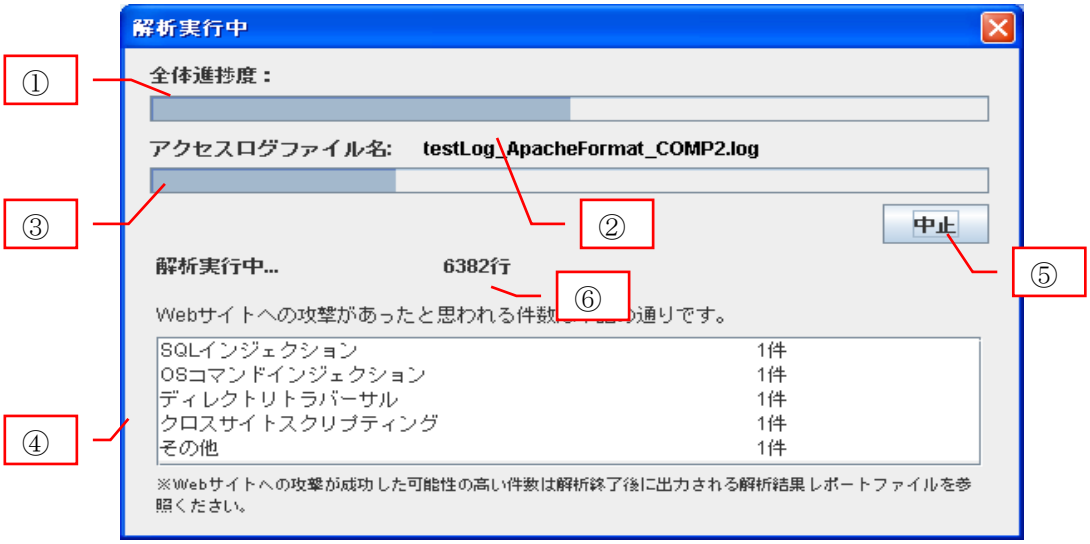
「解析開始」ボタンを押すと、設定の適当性をチェックし、アクセスログ解析が開始されます。正しく設定されていない場合、エラーメッセージを表示し、その後解析は行われません。

3.5. 解析開始

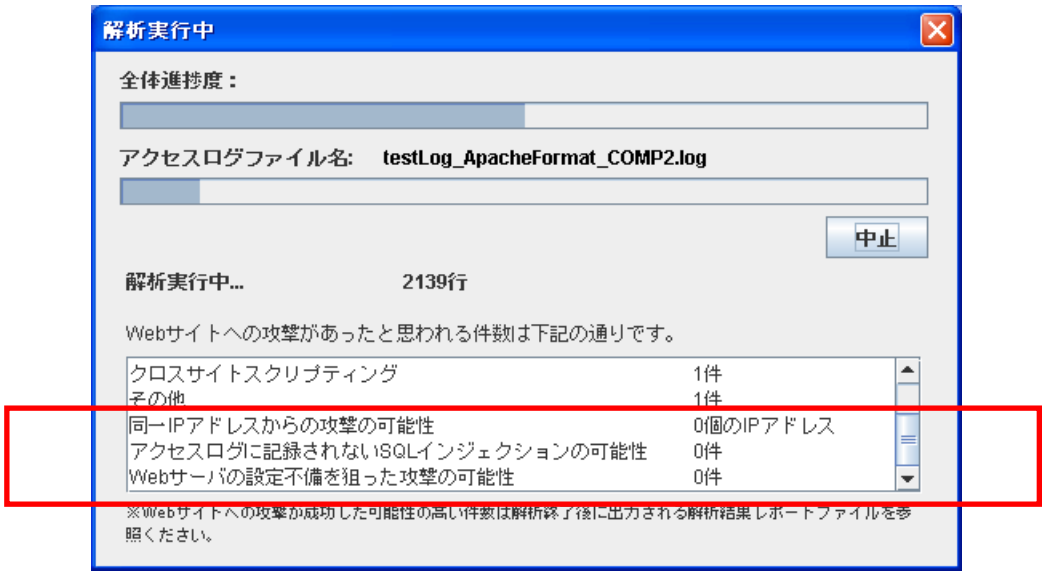
アクセスログファイル形式、解析対象アクセスログファイル、出力先ディレクトリをそれぞれ設定後、解析開始ボタンを押すとアクセスログ解析が開始されます。アクセスログファイル形式、解析対象アクセスログファイル、出力先ディレクトリが全て設定されていない場合、解析は行われません。



アクセスログ解析が開始されると、解析中画面が表示されます。解析中画面では、アクセスログ解析の進捗情報を表示します。①は全体の解析進捗状況が表示されます。②は解析中のファイル名が表示されます。③はファイル単位の解析進捗状況が表示されます。④は、検出対象脆弱性検出数がリアルタイムで表示されます。⑤は解析中止ボタンです。解析を途中で中止したい場合、このボタンを押してください。⑥は解析対象ファイルの解析した行数が表示されます。



解析レベルにて「詳細」を選択した場合、以下のような解析中画面が表示されます。

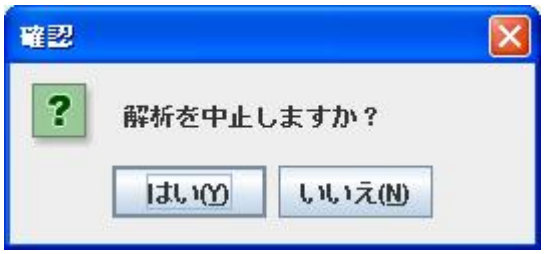


中止ボタンを押した場合、確認ダイアログが表示されます。

確認ダイアログの「はい」を選択した場合、処理を中止しその時点での解析結果が出

力されます。

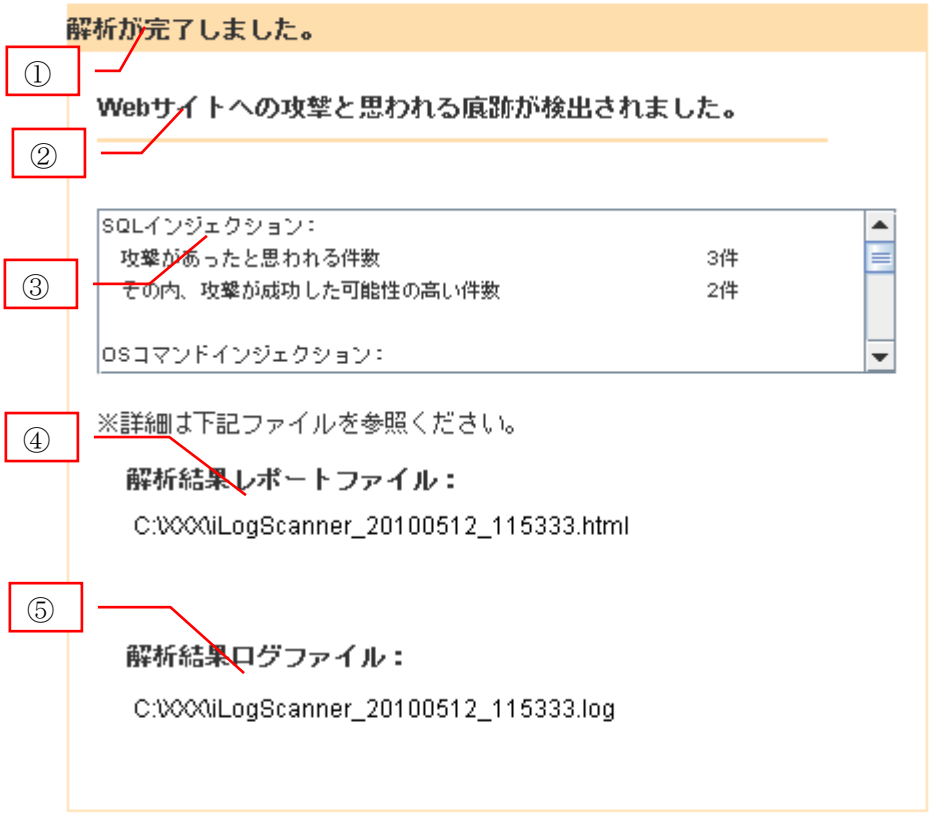
「いいえ」を選択した場合、解析実行中画面に戻ります。



3.6. 解析終了

アクセスログ解析が終了した後、結果ファイル(解析結果レポートファイル、解析結果ログファイル)を作成し、結果画面が表示されます。

【解析結果サマリ画面】



解析結果サマリ画面の①は終了メッセージ(完了/中止)が表示されます。②は攻撃痕跡の有無を示すメッセージが表示されます。③は検出対象脆弱性名と検出数が表示されます。④は結果レポートファイルのパス付ファイル名が表示されます。⑤は結果ログファイル※

のパス付きファイル名が表示されます。

また、アクセスログ解析終了時には、解析結果レポートファイルと解析結果ログファイル※が作成されます。これらの解析結果ファイルは、アクセスログ解析前に指定されたディレクトリに出力されます。

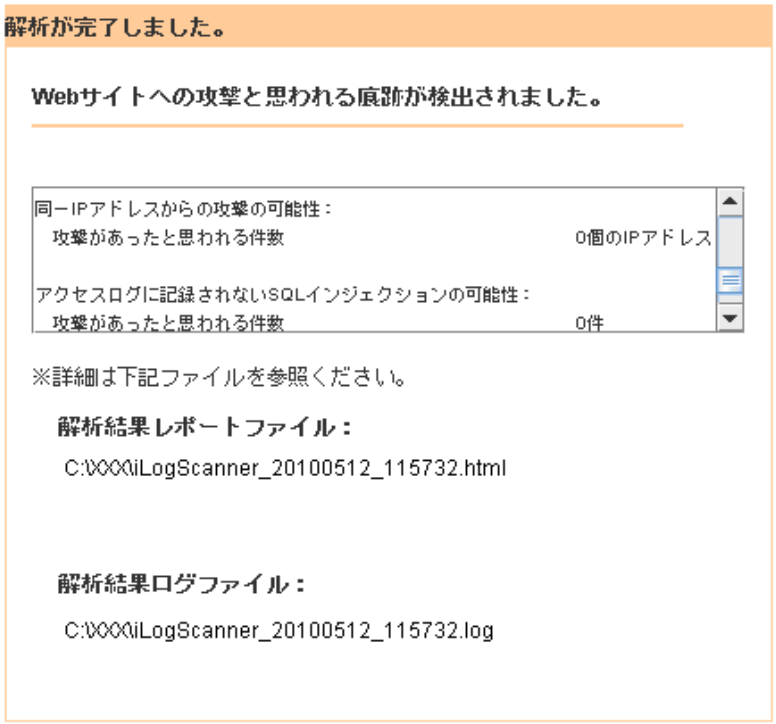
解析結果レポートファイルには解析結果詳細情報が出力され、解析結果ログファイル※には検出したログデータが出力されます。

アクセスログ解析を中止した場合やエラーにより解析中止となった場合は、その時点までの解析結果を出力します。

※解析結果ログファイルは攻撃痕跡を検出した場合のみ出力します。

解析レベルにて「詳細」を選択した場合、以下のような解析結果画面が表示されます。

【解析結果サマリ画面】



3.7. 解析結果レポート

解析結果レポートは、アクセスログ解析終了後、解析前に指定した出力先ディレクトリに出力されます。

解析結果レポートには、解析結果詳細情報と検出対象脆弱性の説明が表示されます。

解析結果情報（上段）では、終了ステータス(完了/中止)、解析日時、解析対象ファイル、解析指定日付、解析対象日付、解析レベル、検出数が表示されます（①は攻撃痕跡を検出した場合のみ表示）。

検出対象脆弱性（下段）では、iLogScanner が検出対象としている脆弱性についての説明が表示されます。対策の詳細については、下記サイトを参照ください。

・IPA　セキュリティセンターの「安全なウェブサイトの作り方」
http://www.ipa.go.jp/security/vuln/websecurity.html

・IPA　セキュリティセンターの「セキュア・プログラミング講座」
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

アクセスログ解析にてウェブサイトへの攻撃痕跡が検出された場合は、製作者またはセキュリティベンダーに相談することをお勧めします。また、ウェブアプリケーションの脆弱性が存在した場合は、脆弱性を放置せず迅速な対策をお勧めします。

解析レベルにて「詳細」を選択した場合、下記のような解析結果レポートが出力されます。

iLogScanner - 解析結果レポート

解析結果

- 終了ステータス：完了
- 解析日時：2010/05/12 11:57
- 解析対象ファイル：testLog_ApacheFormat_COMP1.log, testLog_ApacheFormat_COMP2.log
- 解析指定日付：-
- 解析対象日付：2007/12/12 - 2007/12/12
- 解析レベル：詳細
- 検出数　：計 10 件

検出したWebサイトへの攻撃について、下記に詳細を記述します。

検出対象脆弱性	攻撃があったと思われる件数	攻撃が成功した可能性の高い件数
SQLインジェクション	3	2
OSコマンドインジェクション	2	-
ディレクトリトラバーサル	2	-
クロスサイトスクリプティング	1	-
その他	2	-

詳細レベルで検出したWebサイトへの攻撃について、下記に詳細を記述します。

検出対象項目	攻撃があったと思われる件数
同一IPアドレスからの攻撃の可能性	0
アクセスログに記録されないSQLインジェクションの可能性	0
Webサーバの設定不備を狙った攻撃の可能性	
PUTメソッドの設定不備	0
FrontPage Server Extensionsの設定不備	0
Tomcatの設定不備	0

※痕跡が検出された場合は製作者またはセキュリティベンダーに相談することをお勧めします。
※この結果に該当するアクセスログは「iLogScanner_20100512_115732.log」として確めて保存しています。

検出対象脆弱性の説明と対策

SQLインジェクション

「SQLインジェクション」は、データベースと連携したWebアプリケーションに問合せ命令文の組み立て方法に問題があるとき、Webアプリケーションへ宛てた要求に、悪意を持って細工されたSQL文を埋め込まれて(Injection)しまうと、データベ

・・・中段省略・・・

の攻撃に応じた対策が必要になります。

同一IPアドレスからの攻撃の可能性

同一のIPアドレスからの攻撃痕跡が大量に検出されています。念のため、システムが侵入、悪用されていないかご確認下さい。

本項目の検出基準について、以下に詳細を記述します。

攻撃判定の条件	基準値
同一IPアドレスから同一URL(CGI, ASP, JSP等を含むWebアプリケーション全般)に対する攻撃痕跡が基準値に達している	30件以上
同一IPアドレスからの攻撃痕跡が一定件数に達している	100件以上

アクセスログに記録されないSQLインジェクションの兆候

「アクセスログに記録されないSQLインジェクションの兆候」は、Webサーバが「SQLインジェクション」の攻撃の影響を受けている可能性を示すものです。同一IPアドレスから行われたリクエストに対するWebサーバからのエラー応答が、基準値に達しています。詳細ログより、該当アクセスログが示すWebアプリケーションを参照いただき、問題が生じていないかどうかご確認ください。

本項目の検出基準について、下記に詳細を記述します。

- 条件1：Webサーバの応答コードが5xx番台である
- 条件2：条件1を満たすリクエストが、同一IPアドレスにより行われている
- 条件3：条件2を満たすリクエストが既定時間(30分)内に既定回数(10回)以上行われている

※Webサーバ側のシステム障害(Webサーバとデータベース間の通信障害、データベースの不整合等)やWebアプリケーション側の問題(プログラムが正常動作しない、エラーハンドリングの不足によりプログラムが不正終了している等)にて正常にサービスが提供されていない状態が継続していた場合、本項目が検出される場合があります。詳細ログをご参照いただき、ログに記載された期間にWebサーバが正常稼動していたかどうか等もご確認いただき、問題の有無をご判断ください。

Webサーバの設定不備を狙った攻撃の可能性

Webサーバの設定不備を狙った攻撃を受けている可能性があります。念のため、サーバの設定が意図したものになっている事を確認して下さい。

本項目の検出基準について、下記に詳細を記述します。

対象となる設定不備	攻撃判定基準
PUTメソッドの設定不備	Webサーバの応答コード
FrontPage Server Extensionsの設定不備	特定ファイルへの要求の有無
Tomcatの設定不備	特定ファイルへの要求の有無

Copyright(c) Information-technology Promotion Agency, Japan. All rights reserved

3.8. 解析結果ログ

解析結果ログファイルは、攻撃詳細が記載され、解析結果レポートと同じディレクトリに出力されます。

解析結果ログファイルの形式は以下のとおりです。

```
#解析結果ログの見方
#-----------------------------------------------------------------
#[ログファイル名]
#[行番号] [脆弱性種別] [攻撃が成功した可能性が高い] [該当するアクセスログ] [シグネチャ対応コード]
#-----------------------------------------------------------------
#※ 各項目はタブ区切りになります
#※ 攻撃が成功した可能性が高い場合、「●」がつきます
#以下、解析結果ログ

testLog_ApacheFormat_COMP1.log
    10003    SQLインジェクション      -                YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10013    OSコマンドインジェクション      -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10100    ディレクトリトラバーサル        -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    12999    クロスサイトスクリプティング    -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    17777    その他  -                                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX

testLog_ApacheFormat_COMP2.log
    10003    OSコマンドインジェクション      -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10013    SQLインジェクション     ●                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10100    ディレクトリトラバーサル        -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    12999    SQLインジェクション     ●                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    17777    その他  -                                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
```

①②③④⑤⑥

①は攻撃痕跡を検出したファイル名が出力されます。②は検出したアクセスログの行番号が出力されます。③は検出した脆弱性項目名が出力されます。④は攻撃された可能性が高い場合に「●」が出力されます。⑤は検出されたアクセスログが出力されます。⑥には内部で使用するコードが出力されます。

解析レベルにて「詳細」を選択した場合、以下のような解析結果ログファイルが出力されます。

```
#解析結果ログの見方
#-----------------------------------------------------------------
#[ログファイル名]
#[行番号] [脆弱性種別] [攻撃が成功した可能性が高い] [該当するアクセスログ] [シグネチャ対応コード]
#-----------------------------------------------------------------
#※ 各項目はタブ区切りになります
#※ 攻撃が成功した可能性が高い場合、「●」がつきます
#以下、解析結果ログ

testLog_ApacheFormat_COMP1.log
    10003    SQLインジェクション      -                YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10013    OSコマンドインジェクション      -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10100    ディレクトリトラバーサル        -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    12999    クロスサイトスクリプティング    -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    17777    その他  -                                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX

testLog_ApacheFormat_COMP2.log
    10003    OSコマンドインジェクション      -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10013    SQLインジェクション     ●                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10100    ディレクトリトラバーサル        -         YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    12999    SQLインジェクション     ●                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    17777    その他  -                                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    10013    同一IPアドレスからの攻撃の可能性        100  YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX
    21121    Tomcatの設定不備        -                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    21216    PUTメソッドの設定不備   -                 YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX
    21222    FrontPage Server Extensionsの設定不備  -  YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX XXXX
    21277    アクセスログに記録されないSQLインジェクションの可能性  -  YYYY-MM-DD HH:MI:SS XXXXXXXXXXXXXXX
```

4. iLogScanner ModSecurity 対応機能

iLogScanner ModSecurity 対応機能では、Apache アクセスログファイルおよび ModSecurity のエラーログファイルの解析を行い、解析結果を出力します。

アクセスログ解析のために必要な項目を入力し、解析を実行すると、解析実行中画面が表示され、進捗状況を確認することができます。アクセスログ／エラーログ解析後は、解析結果レポートまたは統計情報レポートを作成し、結果画面が表示されます。

アクセスログファイルのみを指定した場合に、基本の解析を行い、解析結果を出力します。

アクセスログとエラーログ両方とも指定した場合に、アクセスログの基本の解析後、アクセスログの解析結果とエラーログのマッチング機能を実行します。

Apache HTTP Server エラーログファイルのみを指定した場合に、ModSecurity で検出・遮断したデータを解析し、統計情報を出力します。

※ アクセスログ形式は、Apcache1.3 系、Apcache2.0 系、Apcache2.2 系の common タイプのみで対応しております。

※ 解析対象ファイルを複数選択することができません。

4.1. 初期画面表示

iLogScanner トップページの下部にある「次へ」ボタンを押した後、利用規約ページへ遷移します。利用規約内容を確認し、規約に同意される方は「規約に同意して iLogScanner ModSecurity 対応機能版を起動する」ボタンを押して下さい。

「規約に同意して iLogScanner ModSecurity 対応機能版を起動する」ボタンを押した場合、iLogScanner ModSecurity 初期画面が表示されます。

「規約に同意しない」ボタンを押した場合、iLogScanner トップページへ遷移します。

【アクセスログファイル入力画面】

※は必須項目です

解析したいアクセスログファイルを指定してください。

※　どちらか一方、または両方設定してください。

解析対象アクセスログファイル名：

参照...

Apatche 1.3系/2.0系/2.2系のcommonタイプのみ解析可能です。

解析対象 Apatche HTTP Server エラーログファイル名：

参照...

アクセスログ、エラーログのどちらも指定した場合は、アクセスログの解析結果とエラーログのマッチング機能を実行します。
エラーログファイルのみ設定した場合は、攻撃の統計情報を集計する機能[MofSecurityが出力するエラーログの統計]を実行します。
アクセスログのみ指定した場合は、iLogScannerと同様の解析を実行します。
＊iLogScanner ModSecurity対応機能では、複数ファイルの選択は出来ません。

解析結果の出力先ディレクトリを指定してください。

出力先ディレクトリ：※

参照...

下記ファイルの出力先ディレクトリを設定します。
出力するファイルは、実行日をもとにしたファイル名称となります。

・解析結果レポートファイル(iLogScanner_年月日_時分秒.html)
・解析結果ログファイル(iLogScanner_年月日_時分秒.log)
【例】 iLogScanner_20071217_121212.html

注意：同じ名称のファイルがある場合は上書きされます。

解析開始...

詳細内容を指定してください。（任意）

＊指定しない場合、解析レベルは「標準」となります。

オプション...

現在の設定内容
ログフォーマット：-
解析対象範囲　：-
解析レベル　：標準

4.2.　解析対象ファイルの指定

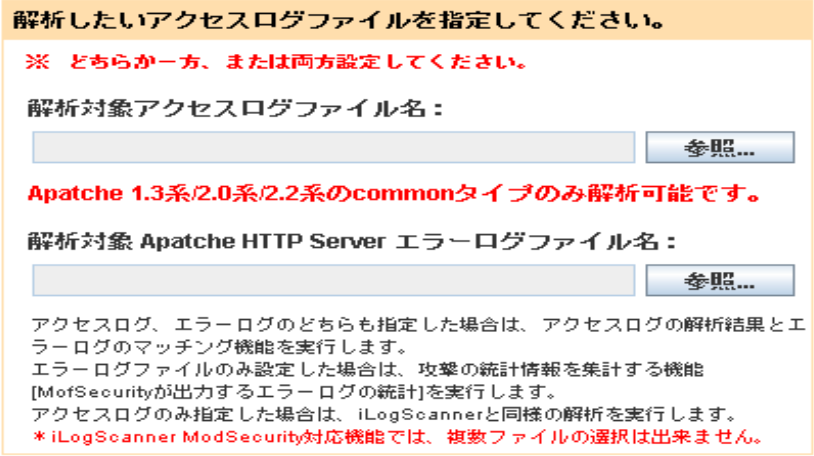
解析を行うアクセスログファイルあるいはエラーログファイルを指定します。

アクセスログについては、「2.5　アクセスログファイル形式」の（3）を参照して下さい。

エラーログについては、「2.6　エラーログファイル形式」を参照して下さい。

(1)　解析対象アクセスログファイルと解析対象エラーログファイル指定

「参照」ボタンを押すと、ファイル選択画面が表示されます。



4.3.　解析結果出力先ディレクトリの指定

「3.3　解析結果出力先ディレクトリの指定」を参照して下さい。

4.4.　オプション指定

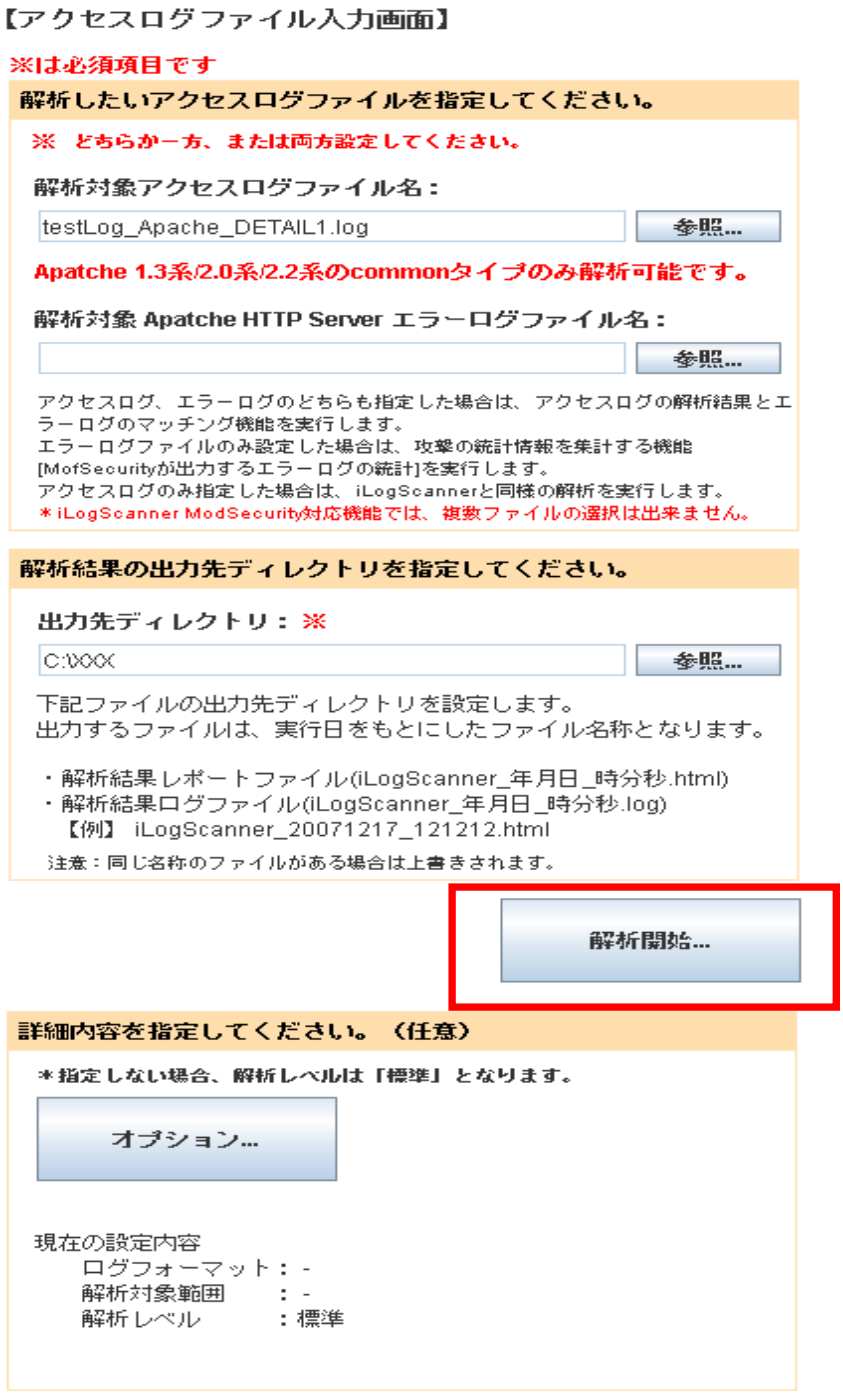
アクセスログファイル／エラーログファイルがいずれ指定されて、また出力先ディレクトリが指定された場合に、「オプション」ボタンを利用できるようになります。

オプション設定画面の操作について、「3.4　オプション設定」を参照して下さい。

※　エラーログファイルのみ指定された場合、オプション設定画面のログフォーマットと解析レベルが利用不可です。

4.5. 解析開始

解析対象アクセスログファイル／エラーログファイル、出力先ディレクトリをそれぞれ設定後、解析開始ボタンを押すと解析が開始されます。解析対象ファイル、出力先ディレクトリが全て設定されていない場合、解析は行われません。

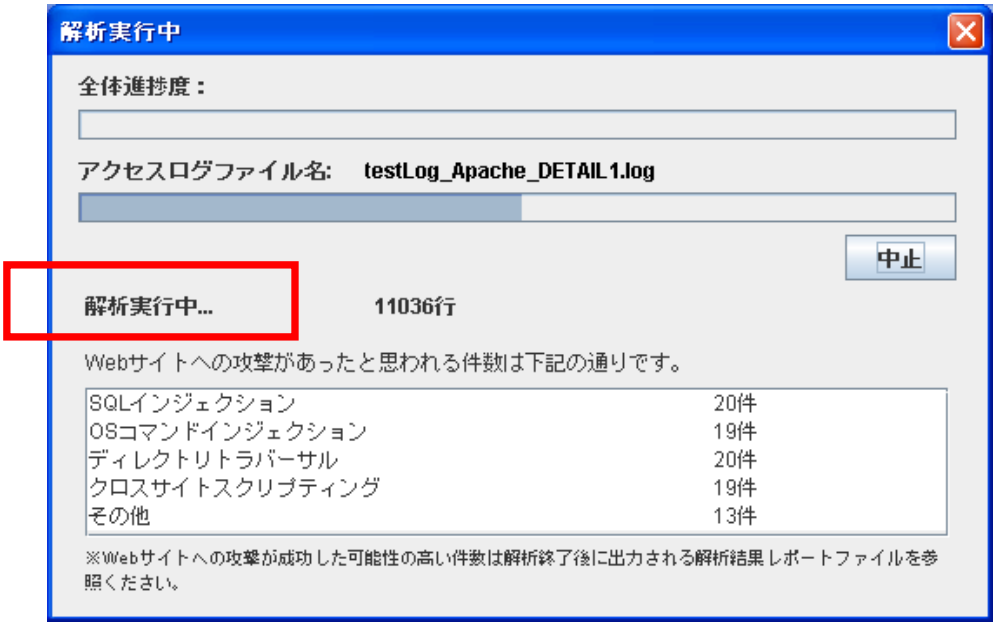


(1) アクセスログファイルのみを指定した場合、解析実行中画面は「3.5 解析開始」

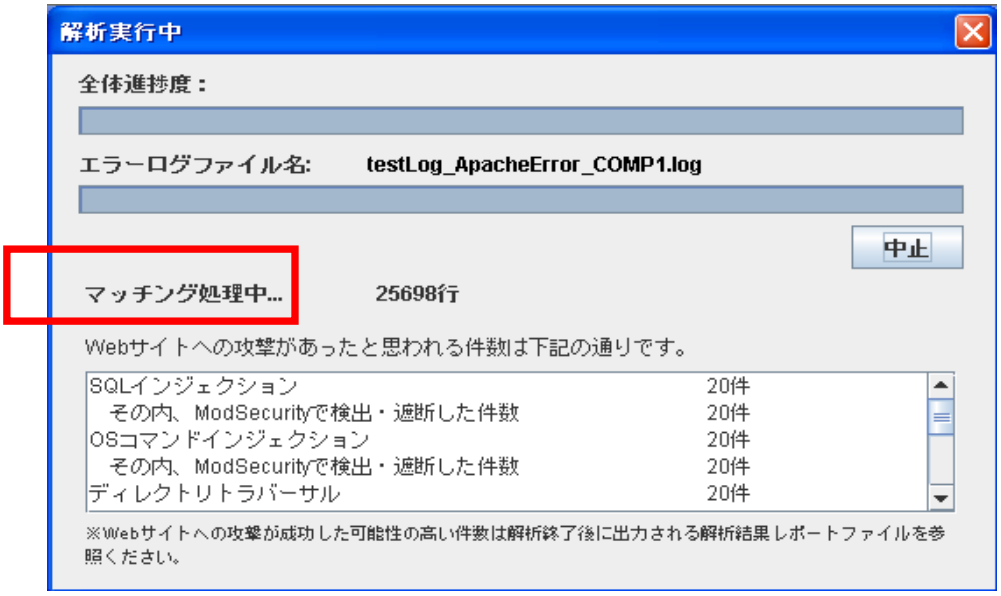
を参照してください。

(2) アクセスログとエラーログファイル両方を指定した場合、解析が開始されると、解析実行中画面は以下の通りに表示します。

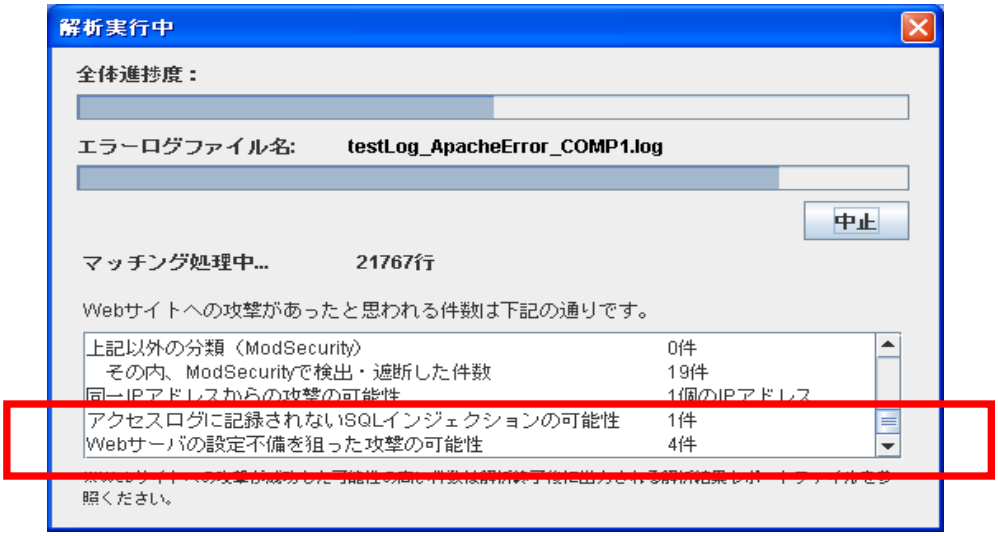
アクセスログファイル解析中



エラーログのマッチング処理中、ModSecurity で検出・遮断した件数が表示されます。

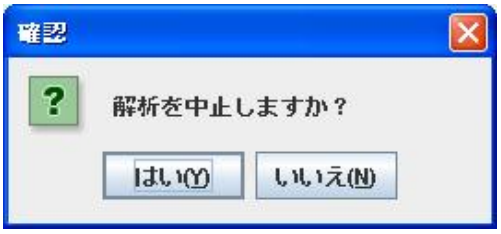


解析レベルにて「詳細」を選択した場合、以下のような画面が表示されます。



(3) エラーログファイルのみを指定した場合、「4.9　ログ統計情報レポート出力」を参照してください。

中止ボタンを押した場合、確認ダイアログが表示されます。確認ダイアログの「はい」を選択した場合、処理を中止しその時点での解析結果が出力されます。「いいえ」を選択した場合、解析実行中画面に戻ります。



4.6. 解析終了

アクセスログ解析が終了した後、結果ファイル(解析結果レポートファイル、解析結果ログファイル)を作成し、結果画面が表示されます。

※ 解析対象エラーログファイルのみで選択した場合、統計情報レポートファイルと統計情報ログファイルを作成します。「4.9 ログ統計情報レポート出力」を参照してください。

【解析結果サマリ画面】

検出対象脆弱性毎、ModSecurity で検出・遮断した件数が表示されます。

SQLインジェクション：
攻撃があったと思われる件数 20件
その内、ModSecurityで検出・遮断した件数 20件
その内、攻撃が成功した可能性の高い件数 0件

OSコマンドインジェクション：
攻撃があったと思われる件数 20件
その内、ModSecurityで検出・遮断した件数 20件

ディレクトリトラバーサル：
攻撃があったと思われる件数 20件
その内、ModSecurityで検出・遮断した件数 20件

クロスサイトスクリプティング：
攻撃があったと思われる件数 20件
その内、ModSecurityで検出・遮断した件数 20件

その他（IDS回避を目的とした攻撃）：
攻撃があったと思われる件数 20件
その内、ModSecurityで検出・遮断した件数 0件

上記以外の分類（ModSecurity）：
攻撃があったと思われる件数 0件
その内、ModSecurityで検出・遮断した件数 20件

解析レベルにて「詳細」を選択した場合、以下のような解析結果画面が表示されます。

【解析結果サマリ画面】

解析が完了しました。

Webサイトへの攻撃と思われる痕跡が検出されました。

アクセスログに記録されないSQLインジェクションの可能性：
　攻撃があったと思われる件数　1件

Webサーバの設定不備を狙った攻撃の可能性：
　攻撃があったと思われる件数　4件

※詳細は下記ファイルを参照ください。

解析結果レポートファイル：
C:\XXX\iLogScanner_20100513_095910.html

解析結果ログファイル：
C:\XXX\iLogScanner_20100513_095910.log

検出対象脆弱性毎、ModSecurity で検出・遮断した件数が表示されます。

SQLインジェクション：
　攻撃があったと思われる件数　20件
　その内、ModSecurityで検出・遮断した件数　20件
　その内、攻撃が成功した可能性の高い件数　0件

OSコマンドインジェクション：
　攻撃があったと思われる件数　20件
　その内、ModSecurityで検出・遮断した件数　20件

ディレクトリトラバーサル：
　攻撃があったと思われる件数　20件
　その内、ModSecurityで検出・遮断した件数　20件

クロスサイトスクリプティング：
　攻撃があったと思われる件数　20件
　その内、ModSecurityで検出・遮断した件数　20件

その他（IDS回避を目的とした攻撃）：
　攻撃があったと思われる件数　20件
　その内、ModSecurityで検出・遮断した件数　0件

上記以外の分類（ModSecurity）：
　攻撃があったと思われる件数　0件
　その内、ModSecurityで検出・遮断した件数　20件

同一IPアドレスからの攻撃の可能性：
　攻撃があったと思われる件数　1個のIPアドレス

アクセスログに記録されないSQLインジェクションの可能性：
　攻撃があったと思われる件数　1件

Webサーバの設定不備を狙った攻撃の可能性：
　攻撃があったと思われる件数　4件

4.7. 解析結果レポート

解析結果レポートは、アクセスログ解析終了後、解析前に指定した出力先ディレクトリに出力されます。

iLogScanner ModSecurity対応機能 - 解析結果レポート

解析結果

- 終了ステータス: 完了
- 解析日時: 2010/05/12 18:37
- 解析対象ファイル: testLog_Apache_DETAIL1.log
- 解析対象エラーログファイル: testLog_ApacheError_COMP1.log
- 解析指定日付: -
- 解析対象日付(アクセスログ): 2010/03/03 - 2010/04/10
- 解析対象日付(エラーログ): 2010/03/30 - 2010/04/07
- 解析レベル: 標準
- 検出数: 計 200 件(ModSecurityで検出・遮断した件数 計 100 件)

検出したWebサイトへの攻撃について、下記に詳細を記述します。

検出対象脆弱性	攻撃があったと思われる件数	その内、ModSecurityで検出・遮断した件数	その内、攻撃が成功した可能性が高い件数
SQLインジェクション	20	20	0
OSコマンドインジェクション	20	20	-
ディレクトリトラバーサル	20	20	-
クロスサイトスクリプティング	20	20	-
その他(IDS回避を目的とした攻撃)	20	-	-
上記以外の分類(ModSecurity)	-	20	-

※痕跡が検出された場合は製作者またはセキュリティベンダーに相談することをお勧めします。
※この結果に該当するアクセスログは「iLogScanner_20100512_183700.log」として確めて保存しています。

検出対象脆弱性の説明と対策

SQLインジェクション

・・・ 中段 省略 ・・・

その他(IDS回避を目的とした攻撃)

16進コード、親パス等の特殊文字を使用して、偽装した攻撃用文字列で攻撃が行われています。これにより、アプリケーションの妥当性チェック機構を迂回し、SQLインジェクション、クロスサイトスクリプティング等の攻撃を行うことを狙ったものです。また、ワームなどが悪用する Web サーバの脆弱性を突いた攻撃でも、このような特殊文字が使われます。それぞれの攻撃に応じた対策が必要になります。

上記以外の分類(ModSecurity)

ModSecurity Coreルールにて下表の"tag"名称を設定していないシグネチャの痕跡を検出した場合、本分類に集計します。下表の"tag"名称に合致する攻撃痕跡は、各脆弱性として集計されます。本分類で検出された攻撃の内容につきましては、詳細ログより該当の"tag"名称を参照いただき、該当のModSecurityのシグネチャのルールをご確認ください。なお、ModSecurity Coreルールにて"tag"名称が未設定のシグネチャが出力するログは、解析対象となりませんのでご注意ください。

検出対象脆弱性	集計対象とする tag 名称
SQLインジェクション	WEB_ATTACK/SQL_INJECTION
OSコマンドインジェクション	WEB_ATTACK/COMMAND_INJECTION
ディレクトリトラバーサル	WEB_ATTACK/FILE_INJECTION
クロスサイトスクリプティング	WEB_ATTACK/XSS WEB_ATTACK/UPDF_XSS

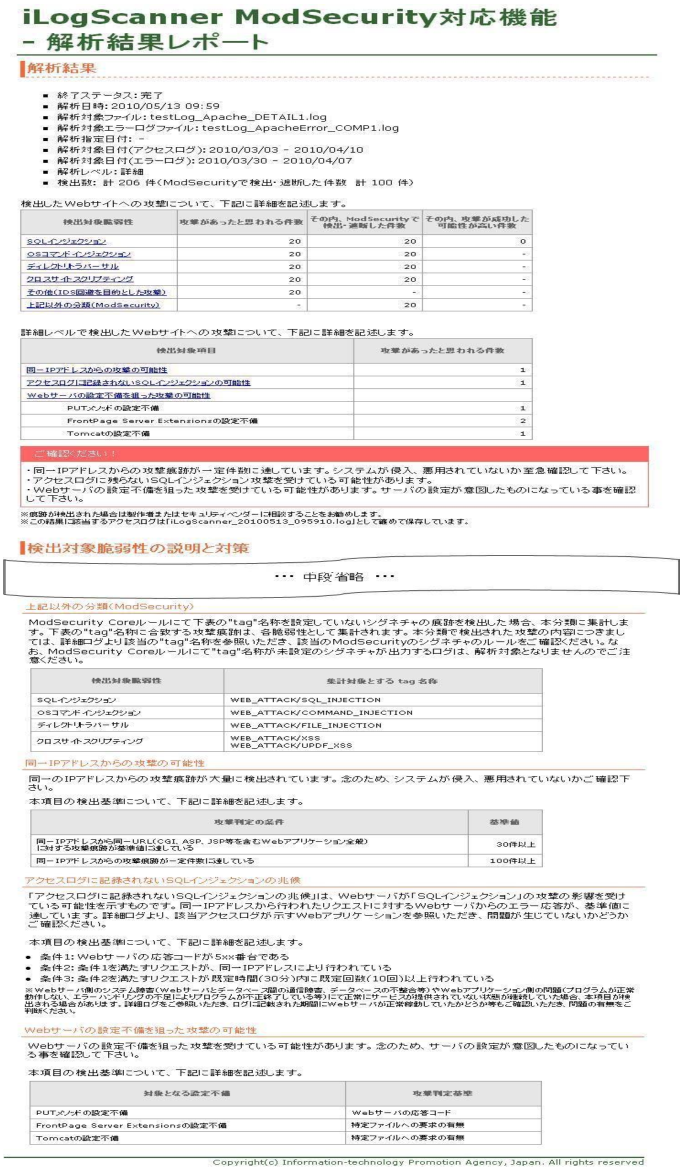
Copyright(c) Information-technology Promotion Agency, Japan. All rights reserved

解析結果レポートには、解析結果詳細情報と検出対象脆弱性の説明が表示されます。

解析結果情報（上段）では、終了ステータス(完了/中止)、解析日時、解析対象ファイル、解析対象エラーログファイル、解析指定日付、アクセスログ／エラーログの対象日付、解析レベル、検出数（ModSecurity で検出・遮断した件数）が表示されます。

検出対象脆弱性（下段）では、iLogScanner ModSecurity が検出対象としている脆弱性についての説明が表示されます。

解析レベルにて「詳細」を選択した場合に、下のような解析結果レポートが出力されます。



iLogScanner ModSecurity対応機能
- 解析結果レポート

解析結果

- 終了ステータス：完了
- 解析日時：2010/05/13 09:59
- 解析対象ファイル：testLog_Apache_DETAIL1.log
- 解析対象エラーログファイル：testLog_ApacheError_COMP1.log
- 解析指定日付：-
- 解析対象日付(アクセスログ)：2010/03/03 - 2010/04/10
- 解析対象日付(エラーログ)：2010/03/30 - 2010/04/07
- 解析レベル：詳細
- 検出数：計 206 件(ModSecurityで検出・遮断した件数　計 100 件)

検出したWebサイトへの攻撃について、下記に詳細を記述します。

検出対象脆弱性	攻撃があったと思われる件数	その内、ModSecurityで検出・遮断した件数	その内、攻撃が成功した可能性が高い件数
SQLインジェクション	20	20	0
OSコマンドインジェクション	20	20	-
ディレクトリトラバーサル	20	20	-
クロスサイトスクリプティング	20	20	-
その他(IDS回避を目的とした攻撃)	20	-	-
上記以外の分類(ModSecurity)	-	20	-

詳細レベルで検出したWebサイトへの攻撃について、下記に詳細を記述します。

検出対象項目	攻撃があったと思われる件数
同一IPアドレスからの攻撃の可能性	1
アクセスログに記録されないSQLインジェクションの可能性	1
Webサーバの設定不備を狙った攻撃の可能性	
PUTメソッドの設定不備	1
FrontPage Server Extensionsの設定不備	2
Tomcatの設定不備	1

ご確認ください！

・同一IPアドレスからの攻撃痕跡が一定件数に達しています。システムが侵入、悪用されていないか至急確認して下さい。
・アクセスログに残らないSQLインジェクション攻撃を受けている可能性があります。
・Webサーバの設定不備を狙った攻撃を受けている可能性があります。サーバの設定が意図したものになっている事を確認して下さい。

※痕跡が検出された場合は製作者またはセキュリティベンダーに相談することをお勧めします。
※この結果に該当するアクセスログは「iLogScanner_20100513_095910.log」として纏めて保存しています。

検出対象脆弱性の説明と対策

・・・ 中段省略 ・・・

上記以外の分類(ModSecurity)

ModSecurity Coreルールにて下表の"tag"名称を設定していないシグネチャの痕跡を検出した場合、本分類に集計します。下表の"tag"名称に合致する攻撃痕跡は、各脆弱性として集計されます。本分類で検出された攻撃の内容につきましては、詳細ログより該当の"tag"名称を参照いただき、該当のModSecurityのシグネチャのルールをご確認ください。なお、ModSecurity Coreルールにて"tag"名称が未設定のシグネチャが出力するログは、解析対象となりませんのでご注意ください。

検出対象脆弱性	集計対象とする tag 名称
SQLインジェクション	WEB_ATTACK/SQL_INJECTION
OSコマンドインジェクション	WEB_ATTACK/COMMAND_INJECTION
ディレクトリトラバーサル	WEB_ATTACK/FILE_INJECTION
クロスサイトスクリプティング	WEB_ATTACK/XSS WEB_ATTACK/UPDF_XSS

同一IPアドレスからの攻撃の可能性

同一のIPアドレスからの攻撃痕跡が大量に検出されています。念のため、システムが侵入、悪用されていないかご確認下さい。

本項目の検出基準について、下記に詳細を記述します。

攻撃判定の条件	基準値
同一IPアドレスから同一URL(CGI、ASP、JSP等を含むWebアプリケーション全般)に対する攻撃痕跡が基準値に達している	30件以上
同一IPアドレスからの攻撃痕跡が一定件数に達している	100件以上

アクセスログに記録されないSQLインジェクションの兆候

「アクセスログに記録されないSQLインジェクションの兆候」は、Webサーバが「SQLインジェクション」の攻撃の影響を受けている可能性を示すものです。同一IPアドレスから行われたリクエストに対するWebサーバからのエラー応答が、基準値に達しています。詳細ログより、該当アクセスログが示すWebアプリケーションを参照いただき、問題が生じていないかどうかご確認ください。

本項目の検出基準について、下記に詳細を記述します。

- 条件1：Webサーバの応答コードが5xx番台である
- 条件2：条件1を満たすリクエストが、同一IPアドレスにより行われている
- 条件3：条件2を満たすリクエストが既定時間(30分)内に既定回数(10回)以上行われている

※Webサーバ側のシステム障害(Webサーバとデータベース間の通信障害、データベースの不整合等)やWebアプリケーション側の問題(プログラムが正常動作しない、エラーハンドリングの不足によりプログラムが不正終了している等)にて正常にサービスが提供されていない状態が継続していた場合、本項目が検出される場合があります。詳細ログをご参照いただき、ログに記載された期間にWebサーバが正常稼動していたかどうか等もご確認いただき、問題の有無をご判断ください。

Webサーバの設定不備を狙った攻撃の可能性

Webサーバの設定不備を狙った攻撃を受けている可能性があります。念のため、サーバの設定が意図したものになっている事を確認して下さい。

本項目の検出基準について、下記に詳細を記述します。

対象となる設定不備	攻撃判定基準
PUTメソッドの設定不備	Webサーバの応答コード
FrontPage Server Extensionsの設定不備	特定ファイルへの要求の有無
Tomcatの設定不備	特定ファイルへの要求の有無

Copyright(c) Information-technology Promotion Agency, Japan. All rights reserved

詳細レベルで検出したウェブサイトへの攻撃について、レポートに詳細を記述し、注意喚起メッセージが表示されます。

4.8.　解析結果ログ

解析結果ログファイルは、攻撃詳細が記載され、解析結果レポートと同じディレクトリに出力されます。

解析結果ログファイルの形式は以下のとおりです。

```
#ModSecurity対応機能 解析結果ログの見方
#-----------------------------------------------------------------
#[ログファイル名]
#[行番号] [脆弱性種別] [[ModSecurityで検知・遮断した][攻撃が成功した可能性が高い][パターン攻撃回数]] [該当するアクセスログ] [シグネチャ対応コード]
#-----------------------------------------------------------------
#※ 各項目はタブ区切りになります
#※ 攻撃が成功した可能性が高い場合、「●」がつきます
#※ ModSecurityで検知したリクエストの場合、「captured」が、遮断したリクエストの場合、「denied」がつきます
#以下、解析結果ログ

testLog_Apache_DETAIL1.log/testLog_ApacheError_COMP1.log
    XXXX    SQLインジェクション          ●          XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    OSコマンドインジェクション   captured   XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    ディレクトリトラバーサル     captured   XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    クロスサイトスクリプティング denied     XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    その他                       -          XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
```

①②③④⑤⑥

①は攻撃痕跡を検出した解析対象ファイル名が出力されます。②は検出したアクセスログの行番号が出力されます。③は検出した脆弱性項目名が出力されます。④は攻撃された可能性が高い場合に「●」が出力されます。※⑤は検出されたアクセスログが出力されます。⑥には内部で使用するコードが出力されます。

解析レベルにて「詳細」を選択した場合に、下のような解析結果ログが出力されます。

```
#ModSecurity対応機能 解析結果ログの見方
#-----------------------------------------------------------------
#[ログファイル名]
#[行番号] [脆弱性種別] [[ModSecurityで検知・遮断した][攻撃が成功した可能性が高い][パターン攻撃回数]] [該当するアクセスログ] [シグネチャ対応コード]
#-----------------------------------------------------------------
#※ 各項目はタブ区切りになります
#※ 攻撃が成功した可能性が高い場合、「●」がつきます
#※ ModSecurityで検知したリクエストの場合、「captured」が、遮断したリクエストの場合、「denied」がつきます
#以下、解析結果ログ

testLog_Apache_DETAIL1.log/testLog_ApacheError_COMP1.log
    XXXX    SQLインジェクション          ●          XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    OSコマンドインジェクション   denied     XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    ディレクトリトラバーサル     denied     XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    クロスサイトスクリプティング captured   XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    その他                       -          XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    同一IPアドレスからの攻撃の可能性                 100    XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX
    XXXX    アクセスログに記録されないSQLインジェクションの可能性 -    XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX
    XXXX    PUTメソッドの設定不備                            -      XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX
    XXXX    FrontPage Server Extensionsの設定不備            -      XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
    XXXX    Tomcatの設定不備                                 -      XXX.XXX.XXX.XXX - -XXXXXXXXXXXXXXXXX XXX XXX   XXXX
```

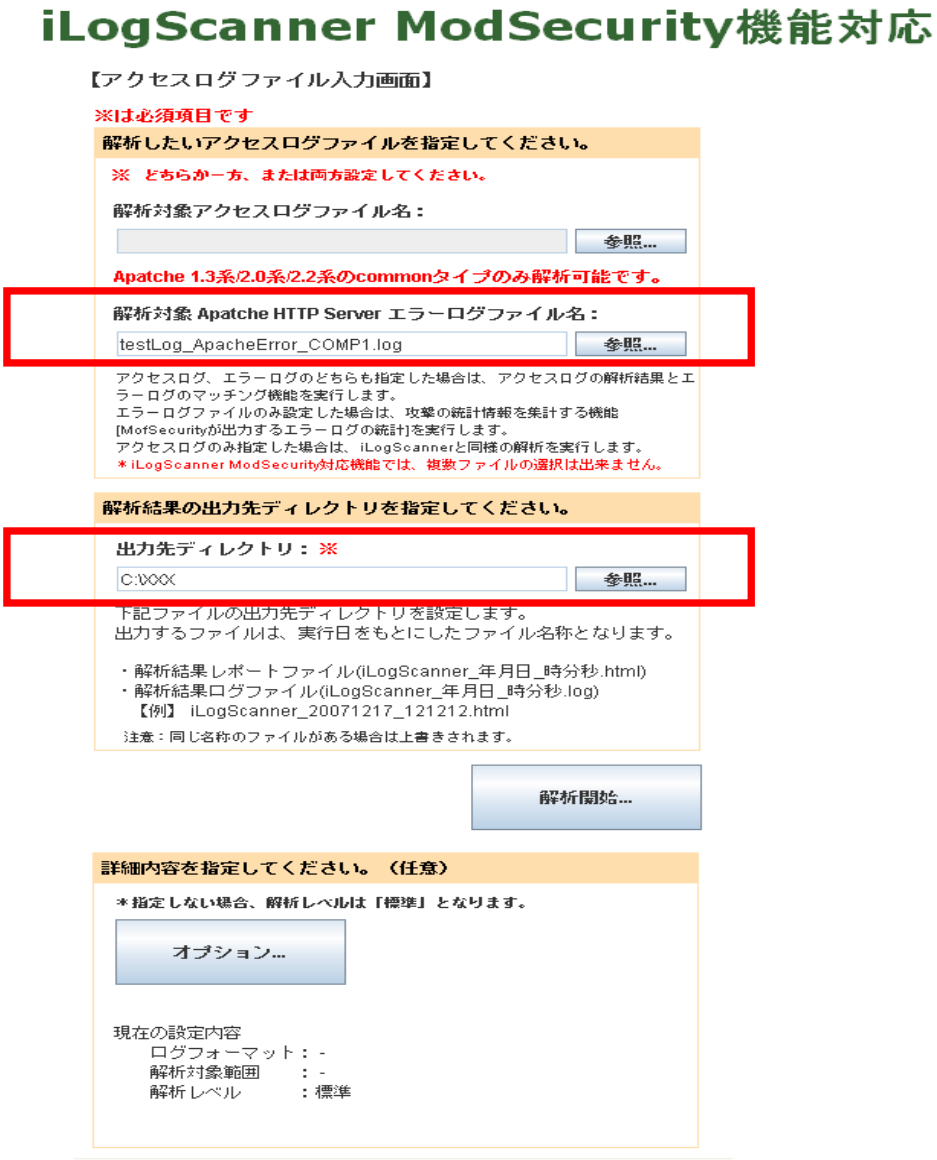
※

※　ModSecurity で遮断した場合、値：「denied」
ModSecurity で検出した場合、値：「captured」
ModSecurity で遮断かどうか不明の場合、値：「deficiency」
攻撃が成功した可能性が高い場合、値：「●」
同一 IP アドレスからの攻撃を検出した場合、検出数を表示　値：「XXX」
攻撃か成功した可能性について不明の場合、値：「-」

4.9. ログ統計情報レポート出力機能

ModSecurity から出力されるエラーログファイルを解析し、攻撃の情報を集計する機能です。解析対象エラーログファイルのみで選択した場合、統計情報レポートファイルと統計情報ログファイルを作成します。ModSecurity で検出・遮断した件数が表示されます。

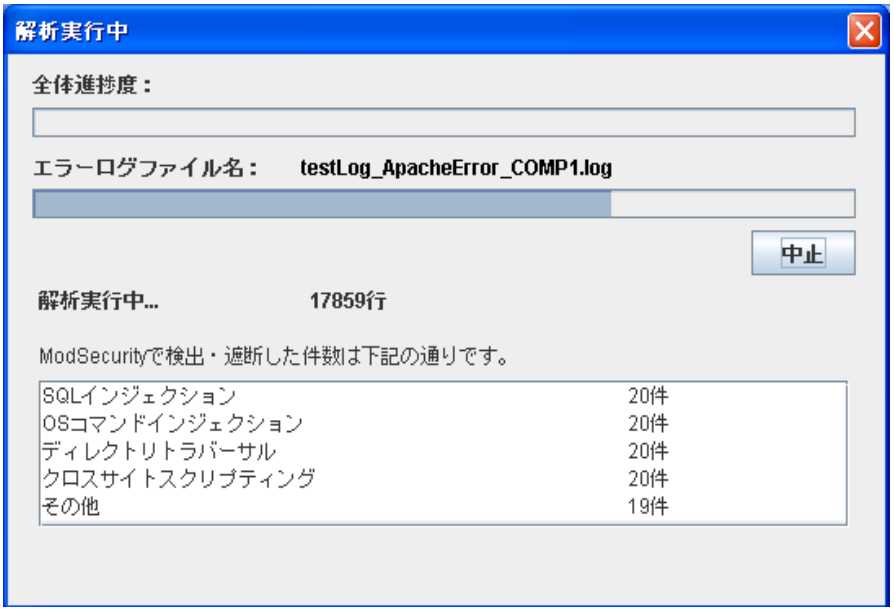
(1) 操作手順



エラーログファイルと出力先ディレクトリを選択後、解析開始ボタンを押すとエラーログ解析が開始されます。選択ファイルが指定された Apache のエラーログ形式ではない場合、解析は行われません。オプション設定画面で集計対象日付を指定することができます。

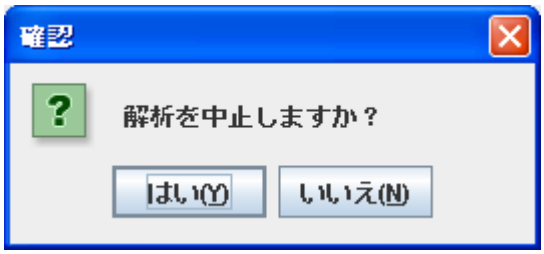
(2)　解析開始

エラーログファイル解析中、ModSecurity で検出・遮断した件数が表示されます。



中止ボタンを押した場合、確認ダイアログが表示されます。

確認ダイアログの「はい」を選択した場合、処理を中止しその時点での統計結果が出力されます。「いいえ」を選択した場合、解析実行中画面に戻ります。



(3)　解析終了

解析が終了した後、結果画面が表示されます。

【解析結果サマリ画面】

検出対象脆弱性毎、ModSecurity で検出・遮断した件数が表示されます。

SQLインジェクション：
　ModSecurityにて検出・遮断した件数　20件

OSコマンドインジェクション：
　ModSecurityにて検出・遮断した件数　20件

ディレクトリトラバーサル：
　ModSecurityにて検出・遮断した件数　20件

クロスサイトスクリプティング：
　ModSecurityにて検出・遮断した件数　20件

その他：
　ModSecurityにて検出・遮断した件数　20件

(4) 統計情報レポート

統計結果レポートは解析前に指定した出力先ディレクトリに出力されます。

iLogScanner ModSecurity対応機能 - 統計情報レポート

解析結果

- 終了ステータス：完了
- 解析日時：2010/04/16 11:21
- 解析対象エラーログファイル：testLog_ApacheError_COMP1.log
- 解析指定日付：－
- 解析対象日付：2010/03/30 - 2010/04/07
- 検出数　：計 100 件

検出したWebサイトへの攻撃について、下記に詳細を記述します。

検出対象脆弱性／ModSecurityエラーログのタグ名称	ModSecurityで検出・遮断した件数
SQLインジェクション	20
WEB_ATTACK/SQL_INJECTION	20
OSコマンドインジェクション	20
WEB_ATTACK/COMMAND_INJECTION	20
ディレクトリトラバーサル	20
WEB_ATTACK/FILE_INJECTION	20
クロスサイトスクリプティング	20
WEB_ATTACK/XSS	11
WEB_ATTACK/UPDF_XSS	9
その他	20
WEB_ATTACK/PHP_INJECTION	10
WEB_ATTACK/SECURITY_INJECTION	3
WEB_ATTACK/OTHER_INJECTION	7

※痕跡が検出された場合は製作者またはセキュリティベンダーに相談することをお勧めします。
※この結果に該当するエラーログは「iLogScanner_20100416_112113.log」として継続で保存しています。

検出対象脆弱性の説明と対策

SQLインジェクション

「SQLインジェクション」は、データベースと連携したWebアプリケーションに問合せ命令文の組み立て方法に問題があると

… 中段省略 …

その他

ModSecurity Coreルールにて下表の"tag"名称を設定していないシグネチャの痕跡を検出した場合、本分類に集計します。下表の"tag"名称に合致する攻撃痕跡は、各脆弱性として集計されます。本分類で検出された攻撃の内容につきましては、詳細ログより該当の"tag"名称を参照いただき、該当のModSecurityのシグネチャのルールをご確認ください。
なお、ModSecurity Coreルールにて"tag"名称が未設定のシグネチャが出力するログは、解析対象となりませんのでご注意ください。

検出対象脆弱性	集計対象とする tag 名称
SQLインジェクション	WEB_ATTACK/SQL_INJECTION
OSコマンドインジェクション	WEB_ATTACK/COMMAND_INJECTION
ディレクトリトラバーサル	WEB_ATTACK/FILE_INJECTION
クロスサイトスクリプティング	WEB_ATTACK/XSS WEB_ATTACK/UPDF_XSS

Copyright(c) Information-technology Promotion Agency, Japan. All rights reserved

統計結果レポート（上段）では、終了ステータス(完了/中止)、解析日時、解析対象エラーログファイル、解析指定日付、解析対象日付、解析レベル、検出数が表示されます。

検出対象脆弱性（下段）では、集計対象としている脆弱性の tag 名称が表示されます。

(5)　統計情報ログ

統計情報ログファイルは、統計結果レポートと同じディレクトリに出力されます。

①

②

③

④

```
#ModSecurity対応機能 統計情報ログの見方
#-----------------------------------------------------------
#[ログファイル名]
#[行番号] [ModSecurityエラーログタグ名称] [-] [該当するエラーログ]
#-----------------------------------------------------------
#※ 各項目はタブ区切りになります

以下、解析結果ログ

testLog_Apache_ModSecurity.log
    XXXX    WEB_ATTACK/SQL_INJECTION        -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/SQL_INJECTION"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
    XXXX    WEB_ATTACK/COMMAND_INJECTION    -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/COMMAND_INJECTION"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
    XXXX    WEB_ATTACK/FILE_INJECTION       -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/FILE_INJECTION"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
    XXXX    WEB_ATTACK/XSS                  -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/XSS"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
    XXXX    WEB_ATTACK/UPDF_XSS             -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/UPDF_XSS"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
    XXXX    WEB_ATTACK/PHP_INJECTION        -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/PHP_INJECTION"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
    XXXX    WEB_ATTACK/SECURITY_INJECTION   -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/SECURITY_INJECTION"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
    XXXX    WEB_ATTACK/OTHER_INJECTION -    [XXX MMM DD HH:MI:SS YYYY] [error] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score.
[file "/XXXXXXXXXXXXXXX"] [line "XXXX"] [msg "XXXXX"] [data "XX"] [severity "XXX"] [tag "WEB_ATTACK/OTHER_INJECTION"] [hostname "XXXXXX"] [uri "/XXXXXXX"] [unique_id "XXXXX"]
```

①は攻撃痕跡を検出したエラーログファイル名が出力されます。②は検出したアクセスログの行番号が出力されます。③は検出した脆弱性の Tag が出力されます。④は検出されたエラーログデータが出力されます。

5. FAQ

iLogScanner に関する FAQ です。

5.1. iLogScannerとは何ですか？

「iLogScanner」は、ウェブサーバのアクセスログからウェブアプリケーション脆弱性を狙った攻撃と思われる痕跡を検出する為のツールです。

今までは特別なスキルが必要だったウェブサーバのアクセスログ解析が、「iLogScanner」を使えば誰でも簡単に行うことができ、今すぐ危険な攻撃と思われる痕跡の有無を確認することが出来ます。

攻撃と思われる痕跡の有無を確認することにより、必要なセキュリティ対策が明らかになります。

- 攻撃と思われる痕跡を全て網羅し、確実に検出するものではありません。また誤検出の場合もあります。
- iLogScanner で攻撃が検出された場合や、特に攻撃が成功した可能性が検出された場合は、ウェブサイトの開発者やセキュリティベンダーに相談されることを推奨します。
- iLogScanner は簡易ツールであり、SQL インジェクション等の攻撃のアクセスログが無ければ脆弱性を検出しません。また、実際の攻撃による脆弱性検査は行っていません。攻撃が検出されない場合でも安心せずに、ウェブサイトの脆弱性検査を行うことを推奨します。
- 解析対象アクセスログ、解析対象エラーログについて、検出が可能な形式がきまっております。必ず、「解析対象のアクセスログ詳細」、「解析対象のエラーログ詳細」をご確認ください。形式が異なる場合、脆弱性の検出が行われない、または脆弱性が検出されません。

ウェブブラウザ上で実行する Java アプレット形式のツールとなっているので、ホームページを見ることができる環境ならば、どこでも簡単に使用することができます。

5.2. iLogScannerは無料で使用できるのですか？

「iLogScanner」は無償で提供され、情報を一切外部に送信することが無いので、手軽にダウンロードして実行することが出来ます。

5.3. iLogScannerが検出できるウェブアプリケーション攻撃の種類を教えてください。

次の脆弱性を狙ったウェブアプリケーション攻撃の痕跡を検出します（2010 年 5 月現在）。

１．SQL インジェクション

2．OS コマンド・インジェクション
3．ディレクトリ・トラバーサル
4．クロスサイト・スクリプティング
5．その他（IDS[3]回避を目的とした攻撃）

また、解析レベルを「詳細」で解析を行うと次のウェブアプリケーションへの攻撃の可能性を検出します（2010 年 5 月現在）。

1．同一 IP アドレスから同一 URL に対する攻撃の可能性
2．アクセスログに記録されない SQL インジェクションの兆候
3．Web サーバの設定不備を狙った攻撃の可能性

- 脆弱性の概要については、「知っていますか？脆弱性（ぜいじゃくせい）」を参照ください。
- 脆弱性の対策については、「安全なウェブサイトの作り方」を参照ください。

5.4. iLogScannerが動作する環境を教えてください。

「iLogScanner」が動作する環境は、次を想定しています。

オペレーティングシステム	Microsoft Windows XP Professional SP3
ウェブブラウザ	Internet Explorer 7
Java 実行環境（JRE）	Sun Microsystems社 J2SE Runtime Environment(JRE) 6.0 （最新版ダウンロード）

その他、次の環境においては一部動作可能であることを確認しております。

- 次に記載した環境での動作を保証するものではございません。オペレーティングシステム/ウェブブラウザ/JRE のバージョン、利用者環境等の違いにより、動作が異なる場合もございますので、予めご了承ください（2010 年 5 月現在）。

	オペレーティングシステム	ウェブブラウザ	Java実行環境（JRE[4]）	動作
1	Microsoft Windows XP	Internet Explorer 6	JRE 6.0	○

[3] IDS：侵入検知システム（Intrusion Detection System）
[4] JRE：Sun Microsystems社 J2SE Runtime Environment

2	Professional SP2	Internet Explorer 7	JRE 6.0	○
3		Internet Explorer 8 Firefox 3	JRE 6.0	○
4			JRE 6.0	○
5	Microsoft Windows XP Professional SP3	Internet Explorer 6	JRE 6.0	○
6		Internet Explorer 7	JRE 6.0	○
7		Internet Explorer 8	JRE 6.0	○
8		Firefox 3	JRE 6.0	○
9	Microsoft Windows7 Professional	Internet Explorer 8	JRE 6.0	○
10		Firefox 3	JRE 6.0	○
11	Microsoft Windows Vista Business ※1	Firefox 3	JRE 6.0	○
12	Linux(CentOS 5)	Firefox 3	JRE 6.0	△※2

○：正常動作する　　△：一部を除き正常動作する　　×：動作しない

※ 1 Windows Vista + Internet Explorer 7 で保護モードが有効の場合、iLog Scanner は正常に動作しません。保護モードを無効にしてしまうと、ブラウザを悪用する不正なソフト（ウイルス、スパイウェア）などの動きを抑えることができなくなってしまいますので、セキュリティの観点から Windows Vista + Internet Explorer 7 上での実行は推奨していません。また、Windows Vista はブラウザが Firefox3 であればユーザの権限に関わらず正常動作します。しかし、Internet Explorer 7（保護モード ON）使用時と比較するとセキュリティ性が高くない為、Firefox での実行は推奨していません。

※ 2 Linux 上で FireFox3 を使用しツールを実行したところ、ModSecurity 版の解析においてアクセスログとエラーログのマージが行われない現象がありました。そのため、Linux 上での実行は推奨しておりません。（ModSecurity 版でのその他の動作（アクセスログ解析と統計情報）は正常に動作しております。）

5.5. 攻撃と思われる痕跡はどのように検出しているのですか？

ウェブサーバのアクセスログに記録されたリクエストのクエリ文字列から、ウェブアプリケーションへの攻撃によく見られる文字列が存在した場合に検出しています。
それぞれの攻撃でよく見られる文字列は次のような意味のある文字列になります。

攻撃種別	文字列
SQL インジェクション	・ SQL ステートメントで使用されるキーワード ・ データベースのシステムテーブル名 ・ SQL ステートメントで使用される関数 ・ システムストアドプロシージャ名 ・ システム拡張ストアドプロシージャ名
OS コマンド・インジェクション	コンピュータの基本ソフトウェアを操作するための命令文やそれらのパラメータ文
ディレクトリ・トラバーサル	ディレクトリ操作文
クロスサイト・スクリプティング	・ スクリプト関数 ・ HTML タグ文字列 ・ イベントハンドラ
その他（IDS[5]回避を目的とした攻撃）	特殊文字を使用して、偽装した文字列

- 一般的な GET メソッドを使用したウェブアプリケーションについて、リクエストのクエリ文字列から攻撃と思われる痕跡を検出しています。
- 一般的な POST メソッドを使用したウェブアプリケーションについては、リクエストのクエリ文字列がアクセスログに出力されない為、攻撃と思われる痕跡を iLogScanner で検出することはできません。
- ウェブアプリケーションへ無差別に攻撃するような一部の攻撃は、 POST メソッドによる攻撃の場合でもリクエストのクエリ文字列がアクセスログに出力される場合がある為、iLogScanner で検出できる場合があります。
- 攻撃が成功した可能性が高いかどうかを検出することができるのは、SQL インジェクションの攻撃と思われる痕跡からのみとなります。

[5] IDS：侵入検知システム（Intrusion Detection System）

5.6. 解析レベルを「詳細」に設定したときに行われる「攻撃が行われている可能性」はどのように検出しているのですか？

オプション選択画面で解析レベルの詳細を選択時、以下 3 項目による解析を行っています。これらは、以下の基準値や条件を設定し、その基準値を超えた場合や条件を満たした場合に攻撃の可能性があると判断しています。また、一部ではウェブサーバのアクセスログに記録されたリクエストのクエリ文字列から、ウェブアプリケーションへの攻撃によく見られる文字列が存在した場合に検出する方法をとっています。

o 同一 IP アドレスから同一 URL に対する攻撃の可能性

攻撃検出用シグネチャによる解析結果に対して、以下の基準にて、再解析を行います。表中の条件を全て満たす場合、攻撃と判断します。

No.	攻撃判定の条件
条件 1	同一 IP アドレスから同一 URL（CGI、ASP、JSP 等を含むウェブアプリケーション全般）に対する攻撃痕跡が一定件数に達している
条件 2	同一 IP アドレスからの攻撃痕跡が一定件数に達している

※標準解析による脆弱性 5 種類の分類は問いません。

o アクセスログに記録されない SQL インジェクションの兆候

アクセスログに次の表中の条件を全て満たすリクエストが記録されている場合、ログに記録されないタイプの SQL インジェクション攻撃が行われた可能性があると判断します。

No.	攻撃判定の条件
条件 1	アクセスログに記録されたリクエストの応答コード （サーバレスポンス）が 5xx 番台であること。 かつ POST メソッドであること
条件 2	条件 1 に合致するリクエストが ・同一 IP アドレスにより ・一定時間以内に規定数回以上行われている

- Web サーバの設定不備を狙った攻撃の可能性

No.	対象	判断基準
1	PUT メソッドの設定不備	リクエストのメソッドが PUT であり、リクエストに対する応答コードが 201 であること
2	FrontPage Server Extensions の設定不備	FrontPage Server Extensions の設定不備を狙うような、特定ファイル URL に対するリクエストが行われていること
3	Tomcat の設定不備	Tomcat の設定不備を狙うような、特定ファイル（URL）に対するリクエストが行われていること

5.7. 攻撃が成功した可能性が高い痕跡はどのように検出しているのですか？

攻撃を受けた際、ウェブサーバのアクセスログに内部エラーが発生したログや攻撃成功時に記録されるログなどの、特徴的なログが記録されている場合、攻撃が成功した可能性が高い痕跡として検出しています。

- ウェブアプリケーションの実装や使用するサーバソフトウェアによっては、アクセスログに特徴的なログが記録されず、攻撃が成功した可能性が高い痕跡を検出できない場合もあります。
- ウェブサーバのアクセスログに記録された攻撃の痕跡は、攻撃を受けたことが記録として残っているのみで、攻撃を受けた結果（攻撃の成功可否）については記録されていません。このため、iLogScanner の解析だけでは、攻撃の成功／失敗について確実な判断をすることはできません。
- 攻撃が成功した可能性が高いかどうかを検出することができるのは、SQL インジェクションの攻撃と思われる痕跡からのみとなります。
- 攻撃が成功した可能性が高い痕跡が検出されない場合でも、攻撃と思われる痕跡が検出された場合は製作者またはセキュリティベンダーに相談することをお勧めします。

5.8. 解析結果で攻撃があったと思われる痕跡が検出されたのですが、どうすればよいですか？

痕跡が検出された場合は、製作者またはセキュリティベンダーに相談することをお勧めします。

- なお、iLogScanner は簡易ツールであり、実際の攻撃による脆弱性検査は行っていません。攻撃が検出されない場合でも安心せずに、ウェブサイトの脆弱性検査を行うことをお勧めします。

5.9. 解析することができるエラーログを出力するModSecurityのバージョンは？

iLogScanner は以下のウェブサーバソフトウェアのエラーログフォーマットに対応しております。

ウェブサーバソフトウェア	エラーログフォーマット
Apache HTTP Server(2.0 系、2.2 系)	ModSecurity2.5 系が出力するエラーログ形式

5.10. 攻撃があったと思われる件数があるのに、その内、ModSecurityで検出・遮断した件数が 0 件なのですがどうしてでしょうか？

1. ModSecurity および Apache のバージョンは iLogScanner が対応しているバージョンになっていますか？

   「5.9. 解析することができるエラーログを出力するModSecurityのバージョンは？」を参照してください。

2. 結果レポートの表の「検出対象脆弱性」項目の「上記以外の分類（ModSecurity)」に検出数が出力されていませんか？

   ModSecurityでエラーログに出力する名称が「iLogScanner」で検出対象としている脆弱性とは異なる場合、結果レポートの表の「検出対象脆弱性」項目の「上記以外の分類（ModSecurity)」に検出数を表示しています。そちらの項目をご確認ください。

3. ModSecurity のルールを設定していますか？

   ModSecurity で遮断／検出するためのルールが設定されているかどうか確認してください。

4. エラーログ出力項目に以下の項目が表示されるように設定されていますか？

   「iLogScanner」で解析処理を行う場合、以下の項目が必須になっています。

   ModSecurity の設定に以下の項目が含まれているかどうかをご確認ください。

   【必須項目】

   - アクセス日時
   - Apache のエラーレベル

- アクセス元 IP アドレス
- タグ
- リクエスト URI
- リクエストの固有番号

5．その他

アクセスログとエラーログが記録している時期が異なる為、マッチングができなかったと言う可能性があります。アクセスログおよびエラーログのデータ内容をご確認ください。

5.11. Javaアプレット画面が表示されませんが、何が原因と考えられますか？

1．JRE がインストールされていますか？

Javaアプレットを動作させるためには、JREが必要になります。Sun Microsystems社のダウンロードサイトから、「J2SE Runtime Environment(JRE) 5.0」をダウンロードしてインストールしてください。

2．インストールされている JRE のバージョンが 5.0 より古いバージョンではないですか？

「iLogScanner」が動作する JRE のバージョンは 5.0 となります。JRE 5.0 をインストールしてください。

3．ウェブブラウザのセキュリティ設定で Java アプレットが起動するように設定されていますか？

「操作手順」の「2.2.ウェブブラウザの設定」を参考にして、Java アプレットが起動するように設定してください。

5.12. 実行中、「入力されたログフォーマットが不正です。」という旨のメッセージが表示されます。どうすればよいですか？

オプション設定画面のアクセスログのフォーマットを入力する項目「ログフォーマット：」に正しく書式指定子が入力されているか、または、必須になっている書式指定子が入力されているかご確認ください。ログフォーマットの詳細については、「操作手順」の「2.5 アクセスログ形式」に記載しております。ご確認ください。

5.13. 実行中、「指定されたディレクトリは、存在しないか書き込み権限がありません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

解析結果の出力先として指定されたディレクトリへの書き込みが許可されていない可能性があります。ディレクトリのセキュリティ設定をご確認ください。

5.14. 実行中、「メモリが不足しています」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

解析するアクセスログファイルに 1 行が非常に大きいログがある場合、Java Plug-in でエラーが発生する場合があります。この場合、Java の起動パラメータ「-Xmx(size)m」を指定して Java が使用するメモリの最大サイズを大きくしてください(デフォルトでは 64MB です)。設定方法の例は「操作手順」の「2.3.Java の設定」をご確認ください。

5.15. 実行中、「システムエラーが発生しました」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

エラーメッセージに記載されているエラーコードをメモとしてお控えいただき、下記のお問合わせ先へご連絡ください。

5.16. 実行画面の表示で英数字以外の文字が全て"□"で表示されてしまいます。どうすればよいですか？利用環境は、Vline Linux4.2/FireFox2.0/JRE5 です。

詳細は、Tips 集に記載しております。「操作手順」の「6.Tips 集」をご確認ください。

5.17. iLogScannerが動作しません。利用環境は、WinXP/Firefox/JRE6 です。どうすればよいですか？

JRE6 のバージョンは新しいでしょうか。

JRE6 の古いバージョンにて FireFox で Java アプレットを起動した際、FireFox がハングアップする現象が確認されております。

JRE6 update20 以降にアップデートしてください。

5.18. 「SQLインジェクションによるホームページ改ざん行為」はiLogScannerで検出できるでしょうか？

「SQL インジェクションによるホームページ改ざん行為」が行われたことを検出することはできません。改ざん行為が行われた可能性が高い痕跡を検出することはできます。

5.19. 検査結果などのデータをIPAに送信していますでしょうか？

現在は、クライアントから IPA へデータの送信は行っておりません。

5.20. 実行中、「ファイルまたはディレクトリが存在していません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

実行途中でファイルまたはディレクトリが消された可能性があります。選択したファイルまたはディレクトリを確認してください。

5.21. 実行中、「入力ファイルのログタイプ形式が不正です。」という旨のメッセージが表示され、解析処理が行われません。どうすればよいですか？

アクセスログまたは、エラーログのログタイプが異なるか、または必須項目が出力されていない可能性があります。アクセスログについての詳細は、「解析対象のアクセスログ詳細」、エラーログについての詳細は「解析対象のエラーログ詳細」をご確認ください。

5.22. 実行中、「入力ファイルに必須のカラムデータが存在していません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

ウェブサーバのアクセスログかどうか今一度ご確認をお願いいたします。また、アクセスログのログタイプが異なるか、必須項目が出力されていない可能性もありますので、ログの項目の確認をお願いいたします。アクセスログについての詳細は、「解析対象のアクセスログ詳細」をご確認ください。

5.23. 実行中、「当ツールを実行する許可が取消しされました。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

実行時に表示された署名確認画面でキャンセルを選択されませんでしたでしょうか。署名確認画面がキャンセルされた場合は、当ツールは実行されません。

※ツール実行時に表示された署名確認画面の署名内容を必ず確認してください。

※一度、ウェブブラウザを閉じ、再度、ウェブブラウザを起動していただく必要があります。

5.24. 解析にはどのくらい時間がかかりますか？

下記に示した環境での計測事例を記載いたします。

※アクセスログを解析レベル標準で解析した結果になります。

- ✓ 観測用アクセスログファイル
  - ➢ IIS5.0/6.0 の W3C 拡張ログファイル形式のアクセスログファイル
    - ・ 全ての行で脆弱性が検出されるアクセスログファイル
      IIS_W3C-1：ファイルサイズ２MB／14446 行（脆弱性 14442 件）
      IIS_W3C-2：ファイルサイズ２MB／7200 行（脆弱性 7196 件）
  - ➢ IIS5.0/6.0 の IIS ログファイル形式のアクセスログファイル
    - ・ 全ての行で脆弱性が検出されるアクセスログファイル
      IIS-1：ファイルサイズ２MB／14336 行（脆弱性 14336 件）
      IIS-2：ファイルサイズ２MB／7200 行（脆弱性 7196 件）

- Apache1.3 系/2.0 系/2.2 系の common 形式のアクセスログファイル
  - 全ての行で脆弱性が検出されるアクセスログファイル
    Apache-1：ファイルサイズ２MB／14616 行（脆弱性 14616 件）
    Apache-2：ファイルサイズ２MB／7192 行（脆弱性 7192 件）

✓ 動作環境

CPU：	Intel Pentium4 2.8GHz
Memory：	1GB
OS：	Microsoft Windows XP Professional SP3
Java ランタイムパラメータ：	最大ヒープサイズ 256MB（-Xmx256m）

✓ 平均処理時間（単位：秒）

- IIS_W3C-1　118.2 秒
- IIS_W3C-2　67 秒
- IIS-1　116 秒
- IIS-2　66 秒
- Apache-1　118.4 秒
- Apache-2　65 秒

※各自の動作させる環境によって時間の差異は発生します。ご了承下さい。

5.25. 今回のバージョンアップで追加した機能は何ですか。

今回のバージョンアップで追加した機能の内容は以下の通りです。

1. より多くの脆弱性を検出できるようになりました。
   - SQL インジェクションの検出パターンを増加
   - OS コマンド・インジェクションの検出パターンを増加
   - クロスサイト・スクリプティングの検出パターンを増加
   - 同一 IP アドレスからの攻撃の可能性
   - アクセスログに記録されない SQL インジェクションの可能性
   - Web サーバの設定不備を狙った攻撃の可能性

2. 解析対象アクセスログを増やしました。
   - IIS5.0/5.1/6.0/7.0 の IIS ログファイルタイプのアクセスログ解析処理の追加

- Apache HTTP Server1.3 系/2.0 系/2.2 系の common タイプのカスタムフォーマット対応

3. ModSecurity2.5 が出力する Apache のエラーログファイルを元に ModSecurity で検出・遮断したデータを解析し、結果レポートを出力する機能を追加しました。

4. 動作する環境を増やしました。
   - Windows7 上での動作確認

6. Tips集

iLogScanner が公開されてからあった問合せのあったものや参考資料を Tips 集として記載しております。（2008 年 11 月現在）

6.1. VlineLinux4.2 + FireFox2.0 +JRE5 においての文字化け対応

VlineLinux4.2 + FireFox2.0 +JRE5 の動作環境において、Java アプレットの日本語表示で英数字以外の文字が全て"□"で表示されてしまう現象の対応方法について、以下に文字化けが解消した事例を記載します。

1．ディレクトリ作成
mkdir /usr/java/jrexxxxx/lib/fonts/fallback
2．ディレクトリ移動して
cd /usr/java/jrexxxxx/lib/fonts/fallback
3．フォントのシンボリックリンクを張る
ln -s /usr/share/fonts/alias/TrueType/*.ttf .
4．Firefox を再起動

参考 URL：http://java.sun.com/j2se/1.5.0/ja/relnotes.html#linux

6.2. IIS7.0 でのW3Cフィールとの設定方法について

IIS6.0 までと IIS7.0 以降で設定方法が変わります。IIS7.0 の設定方法ですが、マイクロソフトの技術情報サイトに詳細な設定方法が記述されています。以下に URL を記載しますのでそちらの情報を参考にしてください。

URL：	http://www.microsoft.com/japan/technet/windowsserver/2008/library/d0de9475-0439-4ec1-8337-2bcedacd15c7.mspx?mfr=true

ウェブサイト攻撃の検出ツール「iLogScanner」取扱説明書

ーウェブサーバのアクセスログを解析して脆弱性を狙った攻撃の検出を簡易に行うツールー

［　発　行　］２００８年　４月１８日 iLogScanner V1.0 版
２００８年１１月１１日 iLogScanner V2.0 版
２０１０年　８月２７日 iLogScanner V3.0 版
［　発行者　］独立行政法人 情報処理推進機構 セキュリティセンター